University of Southern Queensland

Faculty of Health, Engineering & Sciences

Low Cost Passive Radar Through Software Defined Radio

A dissertation submitted by

M.J. Ryan

in fulfilment of the requirements of

ENG4111 and ENG4112 Research Project

towards the degree of

Bachelor of Engineering (Honours) (Electrical & Electronic)

Submitted: October, 2016

Abstract

Passive radars utilise existing terrestrial radio signals, such as those produced by radio or television stations, to track objects within their range. This project aims to determine the suitability of low cost USB TV tuners as hardware receivers for a Software Defined Radio (SDR) based passive radar receiver. Subsequently determining its effectiveness in producing inverse synthetic aperture radar images using data collected from Digital Television signals. Since the initial identification of passive radar, Militaries the world over have been using it as a part of electronic warfare. The evolution of SDR has enabled greater access to the technologies required to implement passive radar, with the greatest limitation being the cost of the required hardware. The availability of low cost hardware was therefore investigated to determine its suitability and subsequently the availability of passive radar to a wider audience.

Research was conducted into the available SDR receivers, and comparison of specifications was made against the low cost receiver used in the project. A functional hardware platform based around the Realtek RTL2832U chipset has been developed to determine its suitability as a low cost receiver verifying its ability to coherently receive radio signals for target identification. A complex ambiguity function was implemented to interpret sampled data windows, with the output of these windows to be compared to the requirements for an inverse synthetic aperture radar input, thus determining the suitability of the device. Interpretation of the received data has identified that although the hardware is capable, a real time implementation of data processing is not yet possible, impeding the ability to determine the suitability of the receiver as an inverse synthetic aperture receiver. The results of testing show that the hardware is capable of receiving and producing radar images, however due to the bandwidth of DVB-T signals , and the bandwidth limitations inherent in RTL-SDR dongles, they have proven not to be suitable for DVB-T based inverse synthetic aperture radar receivers.

University of Southern Queensland

Faculty of Health, Engineering & Sciences

ENG4111/2 *Research Project*

Limitations of Use

The Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences, and the staff of the University of Southern Queensland, do not accept any responsibility for the truth, accuracy or completeness of material contained within or associated with this dissertation.

Persons using all or any part of this material do so at their own risk, and not at the risk of the Council of the University of Southern Queensland, its Faculty of Health, Engineering & Sciences or the staff of the University of Southern Queensland.

This dissertation reports an educational exercise and has no purpose or validity beyond this exercise. The sole purpose of the course pair entitled "Research Project" is to contribute to the overall education within the student's chosen degree program. This document, the associated hardware, software, drawings, and other material set out in the associated appendices should not be used for any other purpose: if they are so used, it is entirely at the risk of the user.

Dean

Faculty of Health, Engineering & Sciences

Certification of Dissertation

I certify that the ideas, designs and experimental work, results, analyses and conclusions set out in this dissertation are entirely my own effort, except where otherwise indicated and acknowledged.

I further certify that the work is original and has not been previously submitted for assessment in any other course or institution, except where specifically stated.

M.J. Ryan

0061010502

Acknowledgments

I would like to acknowledge the following people:

Dr Andrew Maxwell, for his supervision and guidance;

Liam Price, for his supervision, guidance and for sponsoring this project;

Michael Gall, my friend and colleague, for his encouragement throughout the course, for being my competitor, and for helping me get to the end;

my family, friends, and colleagues, who have reviewed and critiqued my dissertation.

my parents, who have been a constant source of encouragement throughout my studies; and

my wife Amy, who is always there for me, and has supported my studies, lived with my bad moods, and has made me the person that I am today.

M.J. Ryan

Contents

List of Tables

List of Figures

Abbreviations

ADC	Analogue to Digital Converter.
ADS-B	Automatic Dependent Surveillance - Broadcast.
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency.
ASK	Amplitude Shift Keying.
BPSK	Binary Phase Shift Keying.
COTS	Commercial Off The Shelf.
CPI	Coherent Processing Interval.
CW	Continuous Wave.
DAB+	Digital Audio Broadcast Plus - Revised format specification.
DAC	Digital to Analogue Converter.
DSO	Digital Storage Oscilloscope.
DSP	Digital Signal Processing.
DVB-T	Digital Video Broadcast - Terrestrial.
EW	Electronic Warfare.
FFT	Fast Fourier Transform.
FM	Frequency Modulated.
FMCW	Frequency Modulated Continuous Wave.
GPS	Global Positioning System.
GSM	Global System for Mobile Communication.

I	In-Phase.
IC	Integrated Circuit.
IEEE	Institute of Electrical and Electronic Engineers.
ISAPBR	Inverse Synthetic Aperture Passive Bistatic RADAR.
ISAR	Inverse Synthetic Aperture RADAR.
ISM	Industrial, Scientific and Medical Radio Frequency Band.
MIMO	Multiple Input - Multiple Output.
MOTS	Military Off The Shelf.
MPC	Multi-Carrier Phase-Coded.
OFDM	Orthogonal Frequency Division Multiplexing.
OOK	On-Off Keying.
PBR	Passive Bistatic RADAR.
PC	Personal Computer.
PISAR	Passive Inverse Synthetic Aperture RADAR.
PLL	Phase Locked Loop.
Q	Quadrature.
QAM	Quadrature Amplitude Modulation.
QPSK	Quadrature Phase Shift Keying.
RADAR	RAdio Detection And Ranging.
RCS	RADAR Cross Section m^2.
RF	Radio Frequency.
RoHS	Reduction of Hazardous Substances.
SAR	Synthetic Aperture RADAR.

SDR	Software Defined Radio.
SNR	Signal to Noise Ratio.
TCXO	Temperature Controlled Crystal Oscillator.
TV	Television.
UMTS	Universal Mobile Telecommunications System.
USB	Universal Serial Bus.
USRP	Universal Software Radio Peripheral.
VCO	Voltage Controlled Oscillator.

List of Units

cm^2	Centimetre Squared (unit of area).
dB	Decibels.
GHz	Gigahertz.
Hz	Hertz.
kHz	Kilohertz.
km	Kilometre.
M	Metres.
m/s	Metre per Second.
mA	Milli-Ampere.
MB	Megabyte.
Mbps	Mega Bits per Second.
MHz	Megahertz.
mm	Millimetres.
Msps	Million Samples per Second.
mW	milli-Watt.
nF	Nanofarad.
ppm	Parts Per Million.

List of Nomenclature

$(S/N)_{min}$	SNR Required for Detection.
B_n	Noise Bandwidth.
C	Speed of Light in a Vacuum.
F_R	Pattern Propagation Factor (Target to Receiver).
F_T	Pattern Propagation Factor (Transmitter to Target).
F_n	Receiver Noise Figure.
G_R	Receiver Antenna Gain.
G_T	Transmitter Antenna Gain.
G	Antenna Gain.
K	Kelvin.
L_R	Receiver Losses.
L_T	Transmitter Losses.
L_{sp}	Signal Processing Losses.
P_T	Transmitter Average Power.
R_M	Maximum Range.
R_R	Target to Receiver Range.
R_T	Transmitter to Target Range.
R	Range.
S_{min}	Minimum Detectable Signal.
T_i	Receiver Input Noise Temperature (K).
V	Velocity.
Δf	Frequency Deviation Present in Modulation Method (Hertz).
λ	Wavelength (m).
ρ	Power Utilisation Factor.
σ_B	Bistatic RADAR Cross Section m^2.
σ	Target RADAR Cross Section.

f_b	Beat Frequency.
f_c	Centre Frequency.
f_m	Rate of Modulation in FMCW Signal.
k	Boltzman's Constant ($1.38 \times 10^{-23} J \cdot K^{-1}$).
t_c	Coherent Processing Interval (CPI) (seconds).

1

Introduction

This chapter provides an overview and background of the dissertation topic, an outline of the objectives of the dissertation, summarising the methodology used to achieve them, a summary of the implications resulting from the outcome of the dissertation, and provides a brief introduction to the subsequent chapters.

1.1 Background

The concept of RAdio Detection And Ranging (RADAR) was first proposed by Heinrich Hertz in the late 19th century and developed over the following decades, with eight nations independently developing their own variations between 1934 and 1939. This initial RADAR development and implementation was achieved using a classic Monostatic RADAR configuration. In the mid 1930's the United Kingdom conducted what has become known as the Daventry experiment (Kuschel & O'Hagan n.d.), this experiment proved that a passive or bistatic RADAR was possible, whereby the transmitter and receiver are not co-located.

Following this implementation Passive Bistatic RADAR (PBR) became part of a standard military Electronic Warfare (EW) suite. Military Off The Shelf (MOTS) implementations of PBR are now available from a number of the larger military component manufacturers, these include the Thales Homeland Alerter 100 (Group 2010) and Lockheed Martin Silent Sentry (Freeman 2007) RADARs.

Whilst Military implementations of PBR have long become a part of a standard EW suite, there are no viable Commercial Off The Shelf (COTS) solutions available to the average user. This hole in the market has been filled by ad-hoc implementations of PBR utilising alternative platforms. The most relevant platform for implementation is Software Defined Radio (SDR), whereby a relatively simplistic hardware receiver is used to provide the In-Phase (I) and Quadrature (Q) signals to a computer for filtering, processing and digestion. Each of the subsequent receiver and demodulation stages undertaken in SDR would have traditionally been implemented through hardware stages and provided to a user interface.

The hardware used to implement a SDR receiver, whilst considerably less expensive

than a MOTS solution, is still priced beyond what could be considered reasonable to the average enthusiast, and hence, not low cost. This changed when Antti Palosaari (Cass 2013) identified that the Realtek RTL2832U chipset based Personal Computer (PC) Television (TV) Tuners were capable of receiving well beyond the range required of a TV tuner and could commonly receive within a range of 24 MHz to 1.7 GHz. Following this discovery, Osmocom, a project group for open source mobile communications with a focus on developing software tools and implementing mobile communications standards, developed an alternative set of drivers which were able to feed the I and Q signals to software developed to decode the radio signals.

This project investigated the suitability of Realtek RTL2832U based USB TV receivers as a hardware interface to a SDR PBR and determined whether inverse synthetic aperture RADAR was plausible with the hardware.

1.2 Outline of the Project

The outline of this study was to determine the suitability of a software defined radio passive bistatic RADAR receiver making use of hardware radio receivers based on the Realtek RTL2832U chipset. A review of existing developments in the field of Passive Bistatic RADAR (PBR) was conducted to determine an appropriate scope and realistic expectations of the hardware devices. A review of existing software developments was conducted to determine the most effective implementation, and a review of existing developments in the use of digital television broadcasts to produce an inverse synthetic aperture RADAR image was conducted. The hardware requirements of a passive bistatic RADAR based upon the Realtek RTL2832U chipset were determined and contrasted against other software defined radio receiver hardware.

1.3 Problem Outline

This dissertation aims to determine the suitability of a low cost software defined radio receiver based upon the Realtek RTL2832U chipset as an interface for an Inverse Synthetic Aperture Passive Bistatic RADAR (ISAPBR).

Testing and evaluation determined a suitable configuration of the hardware receiver, from which a software interface was then developed. The combined hardware and software platforms were tested in both controlled and uncontrolled environments to determine their overall suitability as a viable solution to the problem.

1.4 Research Objectives

The research objectives of this dissertation are derived from the project specification presented in Appendix A.

- Researching bistatic passive RADAR systems and their implementation through software defined radio, the use of Digital Video Broadcast - Terrestrial (DVB-T) broadcast signals to produce an Inverse Synthetic Aperture RADAR (ISAR) output, and use of the Realtek RTL2832u TV tuner as an SDR receiver.

- Development of a suitable test hardware circuit to evaluate the suitability of the RTL28322u receiver for ISAR PBR.

- Development and integration of a software solution to interface the receiver resulting in the production of a RADAR display.

- Testing the circuit and software in a controlled and real world environment, making use of known reference signals to evaluate the performance of the hardware and software in controlled conditions, then validating the circuit with commercial radio sources. The results from each test was evaluated and critically analysed.

- Evaluate the suitability of the Realtek R2832u as the hardware receiver in a Passive Inverse Synthetic Aperture RADAR (PISAR).

The dissertation has the capacity for expansion based upon the available time and resources to include:

- Identification and implementation of improvements in the circuitry and software to increase the reliability and functionality of the RADAR display.

1.5 Methodology Summary

A number of different implementations of passive bistatic RADAR were previously tested in other research, however they were generally proprietary solutions with a price greater than $100,000 AUD (2016), or involved the use of expensive SDR hardware, such as the Universal Software Radio Peripheral (USRP) by Ettus Research (2016*a*). This SDR methodology was demonstrated by the Australian Defence Science and Technology Group (DSTG) at a cost of approximately $60,000 AUD (2014) (Palmer 2014), in contrast, a passive bistatic RADAR configuration based upon devices using the Realtek RTL2832U chipset was estimated to cost less than $1,500 AUD (2016). A literature review was undertaken to understand the current developments in passive bistatic RADAR, and its applications as an inverse synthetic aperture RADAR. From this review it was found that there were no peer reviewed applications of the low cost Realtek RTL2832U chipset based TV Tuner as a software defined passive bistatic RADAR, there-

fore it was determined that further research and testing was required to determine its functionality within this space.

Continuous wave, Frequency Modulated Continuous Wave, and Synthetic Aperture RADAR properties were investigated to determine the most useful type of passive bistatic RADAR. It is necessary to understand the different RADAR definitions, their interactions and subsequently their applications in order to determine the usability of each configuration based on the hardware available. For this research, the configuration of interest focussed on RTL2832U based dongles.

The required hardware design modifications of a RTL-SDR dongle were investigated and tested to optimise the hardware operation for the lowest cost. Once the basic operation of the hardware was confirmed, a Passive Bistatic RADAR (PBR) consisting of a transmitter and receiver that are **not** co-located, was simulated with a doppler RADAR configuration to ensure the hardware function was suitable. Subsequent testing was then carried out with a frequency modulated continuous wave, and then two Orthogonal Frequency Division Multiplexing (OFDM) waves, being that of a Digital Audio Broadcast Plus - Revised format specification (DAB+) radio station, and a Television Broadcast (DVB-T) signal. The results of these tests were evaluated in relation to the:

- suitability of RTL2832U based TV Tuners as PBR receivers;
- suitability of the integrated software platform for producing a RADAR display;
- the functionality of the hardware in a simulated environment;
- the functionality of the hardware using a non-cooperative transmitter; and
- the suitability of the hardware as an inverse synthetic aperture RADAR receiver.

1.6 Project Contributions

There are numerous journal articles outlining the use of software defined radio as a method of receiving and producing a passive bistatic RADAR across all RADAR types. Whilst there is anecdotal evidence to support the use of RTL-SDR hardware as a RADAR, there were no published journals located supporting this hypothesis. This research aimed to determine the suitability of RTL-SDR hardware in producing a PBR and the subsequent application as a hardware receiver for an inverse synthetic aperture RADAR.

1.7 Consequential Effects

Historically, access to RADAR has required substantial and expensive hardware, this has meant that access to the technology has only been viable to those with a sufficient budget. The introduction of software defined radio lessened the cost burden, but still placed it substantially out of reach of a self funded researcher or enthusiast. The discovery of the capabilities of RTL-SDR hardware has further opened access to those with a lower budget. The finding of this research aim to identify the suitability of the RTL-SDR platform as a passive bistatic RADAR receiver and ultimately whether RADAR can now be investigated by almost anyone.

Unfortunately, the byproduct of producing an affordable and accessible RADAR is that it can be accessed by those with nefarious intentions, such as radical militant groups. There is no way to limit access to the technology discussed in this project, however the burden of research and development is that the best intentions are sometimes misused.

Low cost RADAR does, however, have a great number of positive implementations covering a range of military, law enforcement, research, and meteorological uses. Where any existing implementation would require expensive hardware, or a monostatic configuration with licensed transmitters, and an ongoing financial outlay, RTL-SDR based passive RADAR implementations of these same systems, making use of existing transmitters of opportunity, are a substantially lower cost to implement and maintain.

Military applications of PBR include detection of low probability of intercept signals, being signals that are not conducive to interpretation by conventional RADAR, at conventional RADAR frequencies. Low cost passive bistatic RADAR is also capable of detecting stealth targets. This occurs as the stealth technology implemented is designed to deflect specific frequency ranges, hence, using transmitters of opportunity, operating outside of conventional RADAR frequencies, the stealth targets are no longer invisible to RADAR, and become identifiable and trackable.

Passive RADAR also has implementations in the traffic management of aircraft, motor vehicles and people. It can be used to implement air traffic control, for vehicle monitoring in areas of suitable geography, and for border management. With many roads and airports managed by local government bodies, not larger state or federal bodies, the use of passive RADAR receivers significantly reduces the cost borne by the organisation requiring them. The ability to collect this type of data from low cost RTL-SDR based receivers further reduces the cost to organisations.

Similarly, passive bistatic RADAR can be used for weather monitoring over regions that have suitable coverage from a non-cooperative source. Passive bistatic RADAR has been successfully implemented by the French in the form of the Grand Réseau Adapté à la Veille Spatiale (GRAVES) space surveillance system, which transmits a continuous wave frequency of 143.050 MHz and collects the Doppler response from a separate location. The response can also be received on RTL-SDR dongles within a certain geographical area, allowing amateur astronomers to track objects in space.

Dependent upon the intended target for identification by passive bistatic RADAR, public perception and public safety can create problems for the equipment operator. Due to security fears, a large antenna configuration directed at aircraft would raise concerns and attract attention from law enforcement. As a result of this, any passive bistatic RADAR configuration must consider the receiver location requirements, and more so for those seeking to implement RTL-SDR based passive bistatic RADAR for their own knowledge enrichment.

1.8 Risk Assessment

To ensure that the research and experimentation undertaken within this project were safe and appropriate for all involved, it was necessary to identify and manage any and all hazards. Appendix B identifies all of the hazards associated with this project and outlines their subsequent risk management strategy.

Of the hazards identified in Appendix B, there were four (4) with a high risk after additional controls were implemented. The four high risk activities were identified as Soldering whilst making modifications to electronic hardware, Radio Frequency radiation emitted whilst conducting controlled testing, operation of testing equipment in public spaces, and transporting the hardware to a suitable data collection location in a vehicle. These hazards have been outlined below to ensure the associated risk is understood, and an action plan is in place which must be continuously reviewed.

Solder has been identified as a harmful substance, containing lead where the device being modified has not been identified as Reduction of Hazardous Substances (RoHS) compliant. Handling lead and subsequently ingesting it can cause health problems. The flux contained within solder produces arsenic when heated, which can cause health problems if inhaled in a sufficient quantity. The most common control to mitigate the

risks associated with soldering is to work in a well ventilated environment, making use of an extraction fan if necessary. The risk of lead poisoning from solder can be managed by ensuring that after contact with solder, hands are washed before placing them near the face or mouth, and before ingesting any food.

Radio Frequency radiation can cause burns and internal injuries if a person is exposed to a sufficient power level, or for enough time. Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) has identified that for occupational use in the range of 3 kHz to 300 GHz exposure to electromagnetic radiation should not exceed 10 mW/cm^2 (Australian Radiation Protection and Nuclear Saftey Agency 2002, Standards Australia 1998). The United States Federal Communications Commission Part 15 defines that unlicensed wireless equipment operating within the Industrial, Scientific and Medical Radio Frequency Band (ISM) band, within which all testing conducted for this project took place, must not exceed a maximum transmitter power of 30 dBm (1 Watt) (Federal Communications Commission n.d.). By ensuring that all tests were completed using equipment licensed in the ISM band and by using a field strength meter to periodically test the output power of a transmitter, the risk of radio frequency radiation can be reduced.

Operation of the testing equipment comprised of three (3) antennas, and a number of laptops for data processing. Undertaking testing of this nature in a public space presented a problem in terms of public perception. Due to heightened security fears and a constant terrorism threat, it was anticipated that any testing whereby antennas were pointed at aircraft for data collection would result unnecessary concern for the public, and the potential of police intervention. This risk was managed by ensuring all testing was to be undertaken on private property, with the express permission of the property owner, or manager.

The use of a motor vehicle was required in undertaking this project to procure resources and to travel to testing locations where the signal strength is sufficient. This risk was

managed by abiding by all road rules, and ensuring that the driver has undertaken training additional to the standard requirement for a license, such as advanced driver training courses.

1.9 Project Timeline

To ensure that the project was undertaken within the required time frame and meet the objectives of the project specification, a timeline outlining the approximate start and finish dates for each aspect of the project has been developed. Table 1.1 outlines the intended start and finish dates for each element of the project, and the expected time dedicated to each. Appendix C contains a Gantt Chart showing the expected progression through the project.

Project Timeline			
Task	*Start Date*	*Time (Days)*	*End Date*
Realtek RTL2832u SDR Receivers	01 Jan	21	29 Jan
Passive RADAR in Software Defined Radio	01 Feb	44	31 Mar
Digital Video Broadcasts for the implementation of Passive RADAR	25 Mar	25	29 Apr
Project Specification	01 Mar	12	16 Mar
Project Perparedness	01 Mar	12	16 Mar
Project Resources	01 Mar	12	16 Mar
Preliminary Report	01 Apr	38	25 May
Develop Test Circuit	20 Mar	14	7 Apr
Develop and Integrate Software	07 Apr	47	13 June
Verification and Validation of Test Results	13 June	20	11 July
Evaluation of Device Suitability	11 July	10	25 July
Dissertation Development	01 Apr	87	01 Aug
Dissertation Review	01 Aug	45	30 Sep
Dissertation Completion	30 Sep	6	7 Oct

Table 1.1: Resource Allocation: Project Time.

1.10 Resource Requirements

There are a number of resources required to undertake the project. The resource requirements have been categorised and tabulated into the following categories presented in Appendix D:

- Low Cost Passive SDR Hardware Resource Costing (Table D.1);
- SDR Verification Testing Resource Costing (Table D.2);
- WHS Resource Costing (Table D.3); and
- Calibrated Test Equipment (Table D.4).

The tabulated resources contained within Appendix D outline the cost for each line item. The specification and function of each of the components are detailed further within Chapter 4.

1.11 Dissertation Outline

An overview of each subsequent chapter of the dissertation is provided below.

1.11.1 Chapter One – Introduction

This chapter provided an overview and background of the dissertation topic, an outline of the objectives of the dissertation, summarising the methodology used to achieve them, a summary of the implications resulting from the outcome of the dissertation, and provided a brief introduction to the subsequent chapters.

1.11.2 Chapter Two – Literature Review

This chapter provides a comprehensive literature review on passive bistatic RADAR systems, the implementation of PBR through software defined radio, the suitability of DVB-T signals to produce the requisite OFDM encoded Radio Frequency (RF) signal in order to generate an ISAR, and Realtek RTL2832U chipset based SDR receivers.

1.11.3 Chapter Three – Methodology

This chapter presents the methodology used to determine the suitability of the Realtek RTL2832U chipset based receiver as a PBR front end, the testing methodology and verification methodology.

1.11.4 Chapter Four – System Design

This chapter presents the hardware design requirements, components and process required to implement Realtek RTL2832U chipset based devices as PBR receivers in order to achieve the objectives of the project specification.

1.11.5 Chapter Five – Results and Discussion

This chapter presents the results of the hardware analysis in testing the SDR devices under controlled conditions to determine their suitability as a PBR receiver, the results of a controlled RADAR implementation, and the results of field testing, making use of existing terrestrial transmitter sources.

1.11.6 Chapter Six – Further Work

This chapter presents a compendium of research options available to expand the subject research and further develop Realtek RTL2832U chipset based devices as PBR receivers.

1.11.7 Chapter Seven – Conclusions and Recommendations

This chapter summarises the results achieved and compares these to the original project specification objectives. The strengths and weaknesses of assumptions and results are analysed and extrapolated into research that can be undertaken to improve knowledge

in the subject.

2

Background Literature

This chapter provides a comprehensive literature review on passive bistatic RADAR systems, the implementation of Passive Bistatic RADAR (PBR) through software defined radio, the suitability of Digital Video Broadcast - Terrestrial (DVB-T) signals to produce the requisite Orthogonal Frequency Division Multiplexing (OFDM) encoded Radio Frequency (RF) signal in order to generate an Inverse Synthetic Aperture RADAR (ISAR), and Realtek RTL2832U chipset based Software Defined Radio (SDR) receivers.

2.1 Introduction

To undertake any further research on passive bistatic RADAR, its implementation through the use of Digital Television Signals, and the suitability of RTl2832U chipset based devices as a receiver, it is first necessary to undertake a review of existing literature on the topics.

2.2 RADAR

The term RADAR, whilst being recognised within all international English dictionaries as a word, was initially a contraction of RAdio Detection And Ranging. The Oxford English Dictionary (2016) defines RADAR as "A system for detecting the presence of distant objects, and determining their direction, distance, or motion, by transmitting pulses of radio waves or microwaves and detecting or measuring the return of the waves after they have been reflected by the objects." The definition is representative of a monostatic RADAR, being that the transmitter and receiver are co-located and make use of elements of the same hardware for both transmission and reception of radio waves. The concept of RADAR was first explored by Heinrich Hertz in the late 19th century. He proved that radio waves were reflected by metallic objects. Subsequently Thomas Edison filed a patent in 1885 describing a system to avoid collisions at sea based on similar concepts (Stevens 1988).

RADAR is characteristically described by the RADAR range equation. The RADAR range equation relates a number of performance aspects of the RADAR system to other components and their characteristics including:

- transmitted power;
- minimum detectable signal strength;
- gain; and
- RADAR Cross Section m^2 (RCS).

The equation contrasts the different elements that comprise a RADAR and identifies any compromises that may be made in order to design a functional system. The characteristic RADAR range equation was defined by Faulconbridge (2002) as:

$$R_M = \left[\frac{P_T \times G^2 \times \lambda^2 \times \sigma}{(4\pi)^3 \times S_{min}} \right]^{\frac{1}{4}} \tag{2.1}$$

where:

P_T	Transmitter Average Power
G	Antenna Gain
λ	Wavelength (Metres)
σ	Target Cross Section (m^2)
S_{min}	Minimum Detectable Signal

further, the minimum detectable signal is calculated as:

$$S_{min} = k \times T_i \times B_n \times F_n \times (S/N)_{min} \tag{2.2}$$

where:

k	Boltzman's Constant ($1.38 \times 10^{-23} J \cdot K^{-1}$)
T_i	Receiver Input Noise Temperature (K)
B_n	Noise Bandwidth
F_n	Receiver Noise Figure
$(S/N)_{min}$	SNR Required for Detection

Finally, the noise bandwidth is defined as:

$$B_n = \frac{1}{\tau} \tag{2.3}$$

where τ is the pulse width of an impulse RADAR. The relationship between the coefficients of the Monostatic RADAR ranging equation and the PBR ranging equation will be explored in subsequent Chapters of the research.

2.2.1 RADAR Topologies

There are three (3) major RADAR topologies used. These are; monostatic, bistatic and multistatic. The primary focus of this dissertation was bistatic RADAR, however it is necessary to define and understand a number of monostatic RADAR concepts in order to adequately explain bistatic RADAR.

2.2.1.1 Monostatic RADAR

The term "Monostatic RADAR" is used to describe the most common type of RADAR in which the transmitter and receiver are co-located, with elements of the transmitter and receiver hardware being shared. A simplified topology of monostatic RADAR is shown in Figure 2.1. Whilst not the subject topology of this dissertation, as the initially developed and most widely utilised topology, many concepts and definitions are derivative of the monostatic RADAR concepts.

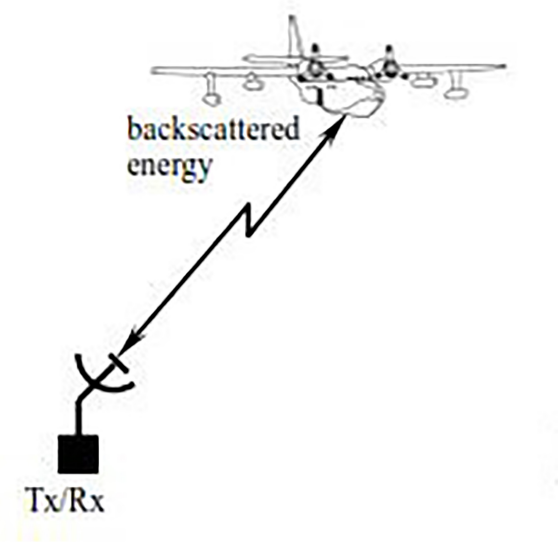


Figure 2.1: Simplified monostatic RADAR topology (Anker 2016).

2.2.1.2 Bistatic RADAR

The term "Bistatic RADAR" is used to describe a RADAR in which the transmitter and receiver are in different locations. It is generalised that the term is used to describe a RADAR whereby the separation distance between the transmitter and receiver is

equal to that of the expected target difference, however this does not apply exclusively. There are a number of benefits afforded to a bistatic RADAR configuration that are not available with a monostatic configuration. these include, but are not limited to:

- no requirement for a transmitter;
- a receiver location away from the transmitter;
- no radio signature produced when interrogating targets; and
- the ability to use low cost receivers with existing terrestrial transmitters.

A simplified topology of a bistatic RADAR is shown in Figure 2.2.

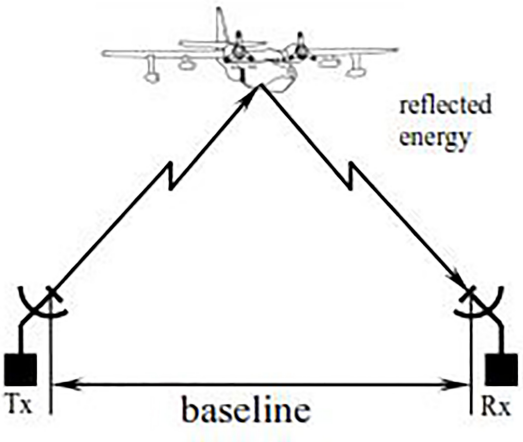


Figure 2.2: Simplified bistatic RADAR topology (Anker 2016).

2.2.1.3 Multistatic RADAR

The term "Multistatic RADAR" is an expansion of the bistatic RADAR concept employing multiple receivers to produce an image of either greater accuracy, or covering a larger surface area. Multistatic RADAR should not be confused with Multiple Input -

Multiple Output (MIMO) RADAR which is the use of multiple transmitter and receiver sites. The definition of multistatic RADAR is included for completeness, however this dissertation will not expand to cover the multistatic RADAR. A topology diagram is included in Figure 2.3.

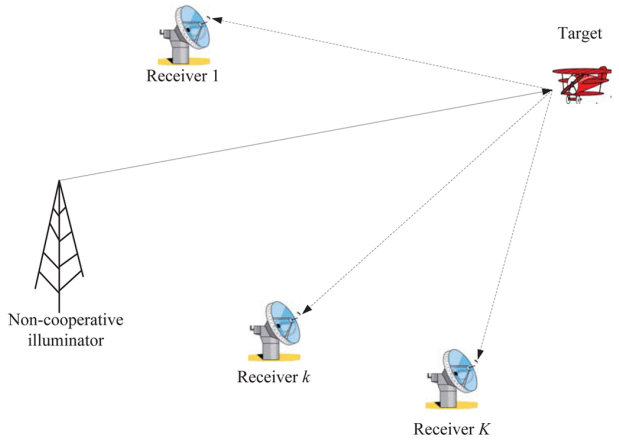


Figure 2.3: Simplified multistatic RADAR topology (Liu et al. 2014).

2.2.2 RADAR Propagation Methods

There are three (3) primary ways in which a radio wave can be transmitted and subsequently used to produce a RADAR image. These are; Continuous Wave (CW) RADAR, Impulse RADAR, and Frequency Modulated Continuous Wave (FMCW) RADAR.

2.2.2.1 Continuous Wave RADAR

Continuous wave RADAR operates by transmitting a known stable frequency of continuous wave radio energy which is then reflected off objects and received. Whilst the term continuous wave RADAR is applicable to any RADAR that relies on a continuous waveform, irrespective of modulation, this research will refer to any unmodulated contin-

uous wave RADAR by the term continuous wave RADAR. An unmodulated continuous wave RADAR is reliant upon a signal of the general form shown in equation 2.4 or the equivalent equations for triangular or square generated waveforms.

$$y(t) = A\sin(2\pi ft \ + \ \varphi) \tag{2.4}$$

where A is the amplitude, f is the angular frequency of the wave and φ is the phase. Figure 2.4 shows the basic block layout of a continuous wave RADAR.

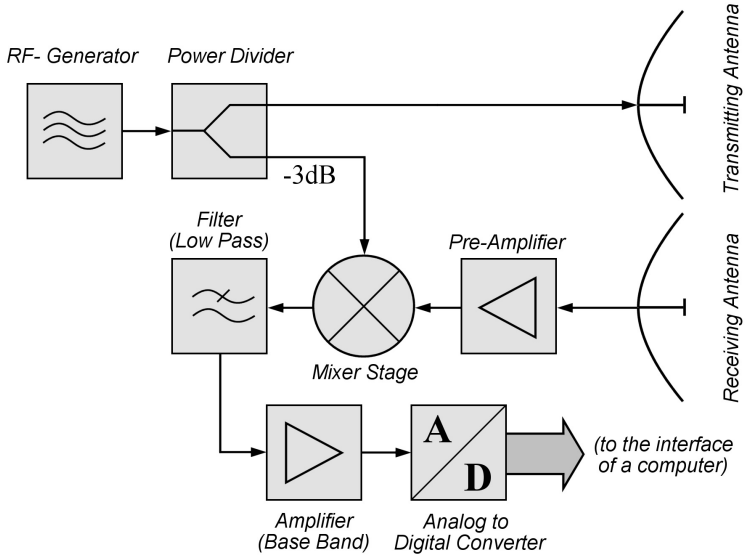


Figure 2.4: Continuous Wave RADAR Block Diagram (Whisky 2012).

In its simplest form unmodulated continuous wave RADAR return frequencies are shifted away from the transmitter frequency based on the Doppler effect. An unmodulated continuous wave RADAR is only functional with moving objects and is capable of determining the velocity at which the target is arriving toward or departing from the RADAR. An unmodulated continuous wave RADAR is not capable of evaluating distance, hence it is primarily used for the evaluation of speed.

The doppler frequency change is dependent on the speed of light C and the velocity of

the target V such that:

$$f_r = f_t \left(\frac{1 + V/C}{1 - V/C} \right) \tag{2.5}$$

Therefore the Doppler frequency as defined by Ridenour (1947) is:

$$f_d = f_r - f_t = 2V \frac{f_t}{(C - V)} \tag{2.6}$$

An unmodulated continuous wave RADAR is only capable of detecting moving targets. Stationary targets within its line of sight will not cause a Doppler shift. The reflected signal from stationary and slow moving targets is substantially similar to the transmitted signal, in that the Doppler shift is insignificant, and is therefore generally overwhelmed by the transmitted signal and indistinguishable to the receiver.

For passive bistatic RADAR the Doppler equation is defined differently. Brown (2013) showed that the Doppler shift is proportional to the rate of change of bistatic range:

$$f = \frac{1}{C} \frac{d}{dt} (R_T + R_R) \tag{2.7}$$

where R_T and R_R can be calculated by:

$$R = \frac{Distance}{3 \times 10^8} \tag{2.8}$$

based on the assumption that the illuminator of interest is travelling at the speed of light in free space, 3×10^8.

2.2.2.2 Frequency Modulated Continuous Wave RADAR

Frequency Modulated Continuous Wave (FMCW) RADAR expands on the initial concept of a continuous wave RADAR by allowing target range to be acquired. CW RADAR cannot determine a target's range as it does not have a timing mark upon which an accurate measure of the transmit and receive cycle time can be gauged. Another benefit of an FMCW RADAR is that it is capable of identifying targets that are stationary.

The function of an FMCW RADAR is otherwise similar to that of a standard CW RADAR and in the same way CW RADAR is limited, an FMCW radar is limited in that it can only accurately track a single target at any time. An FMCW RADAR is able to operate from any type of modulated source, this can include an analogue Frequency Modulated (FM) radio transmitter, or any of the more recently introduced digital transmitters such as Digital Broadcast Television, Digital Audio Broadcast Radio, Mobile Telephones, Wi-Fi, and Wi-Max.

The range of a target identified by FMCW RADAR was determined by Faulconbridge (2002) to be calculated as:

$$R = \frac{f_b \times C}{4 \times \Delta f \times f_m} \tag{2.9}$$

where R is the target range in metres, f_b is the beat frequency due to target range in Hertz, Δf is the frequency deviation present in the modulation method in Hertz, and f_m is the rate of modulation in the FMCW signal in Hertz.

2.2.2.3 Synthetic Aperture RADAR

Synthetic Aperture RADAR (SAR) is generally utilised on moving platforms to simulate a larger antenna aperture. Its function is similar to that of a phased-array antenna, except that instead of utilising a large physical antenna area, a small antenna is used. Successive results are stored and combined to produce a high resolution image of an area. Synthetic aperture RADAR was developed in 1951 by Carl Wiley (Carrara, Goodman & Majewski 1995). The improvement in azimuth resolution and the range resolution of large bandwidth pulses allow the production of SAR images where the reflectivity of the scene is represented by the intensity of each pixel.

There are two common SAR data acquisition modes, strip-map and spotlight. In strip-map mode, the beam location remains constant and observes a strip of area parallel to its movement. Spotlight mode keeps the RADAR beam fixed at the centre of a scene during collection (Gutierrez del Arroyo 2012). Figure 2.5 depicts the spotlight synthetic aperture RADAR collection mode.

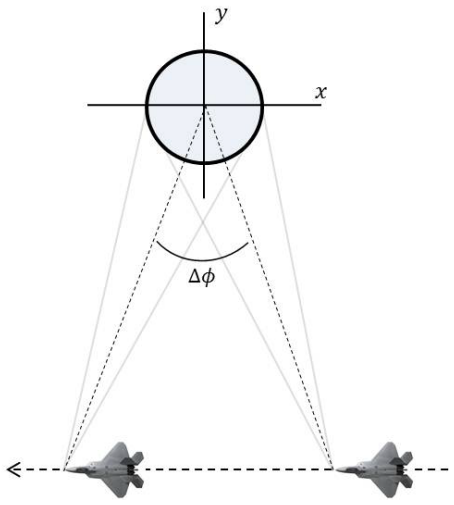


Figure 2.5: Spotlight SAR Collection Mode (Gutierrez del Arroyo 2012).

.

The spotlight method of SAR data acquisition most accurately replicates the opposite of the inverse synthetic aperture RADAR collection method, and is hence further detailed. Monostatic spotlight SAR imaging along the y axis was defined by Gutierrez del Arroyo (2012) as:

$$\rho_y = \frac{C}{2B} \tag{2.10}$$

and along the x axis as:

$$\rho x = \frac{\lambda}{2\Delta\phi} \tag{2.11}$$

where C is the speed of light in metres per second, B is the pulse bandwidth in Hertz, λ is the pulse wavelength in metres, and $\Delta\phi$ is the azimuth collection in radians.

The collected data is compressed or filtered, then subsequently sampled in what is known as fast time samples, being the RADAR image calculation resolution. The transmission time of each pulse defines slow time, the rate at which the acquisition vehicle passes over the collection range.

The slow time and fast time data samples are arranged into a two dimensional array in the frequency domain before being processed to form an image. Two of the most common methods for processing the data are the polar formatting algorithm and the convolution back projection algorithm. Further details on the processing of SAR images can be found in Ozdemir (2012).

2.2.2.4 Inverse Synthetic Aperture RADAR

The Synthetic Aperture RADAR (SAR) described in Section 2.2.2.3, is reliant upon the RADAR antenna moving in order to acquire a comparatively stationary target. In order to implement a SAR on a system where the RADAR antenna is stationary relative to the target, it is necessary to use the inverse SAR technique. ISAR is commonly implemented against ships that are moving in three dimensions (roll, pitch, and yaw) on the ocean's surface, or for tracking aircraft moving across the sky.

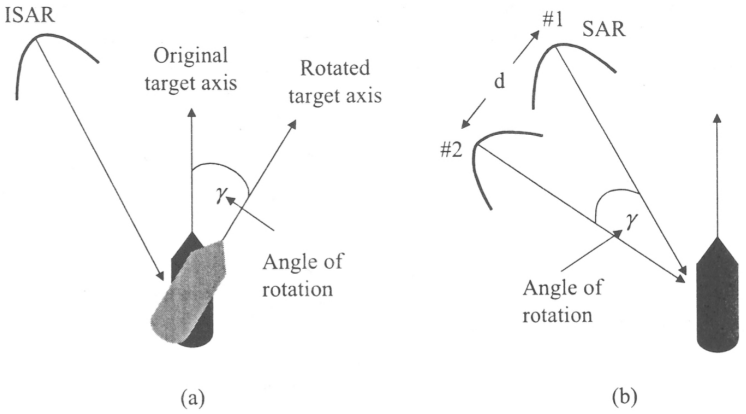


Figure 2.6: Comparison between (a) ISAR and (b) SAR techniques (Faulconbridge 2002).

The concept of ISAR was illustrated by Faulconbridge (2002) in Figure 2.6 comparing an ISAR technique with the conventional SAR technique. Faulconbridge (2002) stated that in Figure 2.6 (a), the target rotates by an angle γ to provide a relative movement between the RADAR and target. When viewed from the target's perspective, the movement is equivalent to the movement made by the RADAR from point #1 to point #2, as shown in Figure 2.6 (b). The distance d in metres between points #1 and #2 becomes a function of the angle of rotation γ in radians and the target range R, therefore:

$$d = \gamma \times R \tag{2.12}$$

Inverse synthetic aperture RADAR is primarily used in maritime surveillance applications, whereby, an aircraft overflies a region of water repeatedly in order to acquire an accurate picture of the space. ISAR can also be used in terrestrial applications, however, as multiple passes over a target region are required, producing an accurate picture of rapidly moving targets, such as aircraft, is not plausible. ISAR can be used similarly over land as it can water, and is commonly used to produce terrain maps.

More recently, ISAR has been used to produce terrain maps of asteroids in deep space. With appropriate range and velocity data, it is possible to produce an ISAR image of any region or target, hence RTL-SDR dongles will be investigated for their suitability as an ISAR receiver.

2.2.3 Passive Bistatic RADAR

Passive Bistatic RADAR (PBR) is primarily implemented in two distinct ways; Installations where both the transmitter and receiver are controlled, or installations where the receiver is controlled, and the transmitter is classified using the interchangeable terms of either "opportunistic" or "non-cooperative." The terms essentially refer to a transmitter source that is generally a commercial broadcast, or any other suitable extant transmission in the geographical area of interest.

The concept behind PBR is similar to that of a Monostatic RADAR in that it compares the transmitted signal with a returned signal to identify scattering and therefore the position and velocity of potential targets. A Monostatic RADAR receives a direct feed of the transmitted signal, however, a PBR requires a minimum of two receivers to achieve this: One to receive a direct-path from the transmitter, and another to receive the scattered return signal containing target information. Additional receivers can be used to add direction finding capabilities to the RADAR if required. Implementation of a PBR requires only simple receivers such as the RTL2832U based TV tuner with the

burden transferred to Digital Signal Processing (DSP).

Figure 2.7 shows a functional diagram of the implementation of passive bistatic RADAR. The diagram identifies the requirement for coherent receivers sharing a single clock source, and identifies the relevant signal paths.

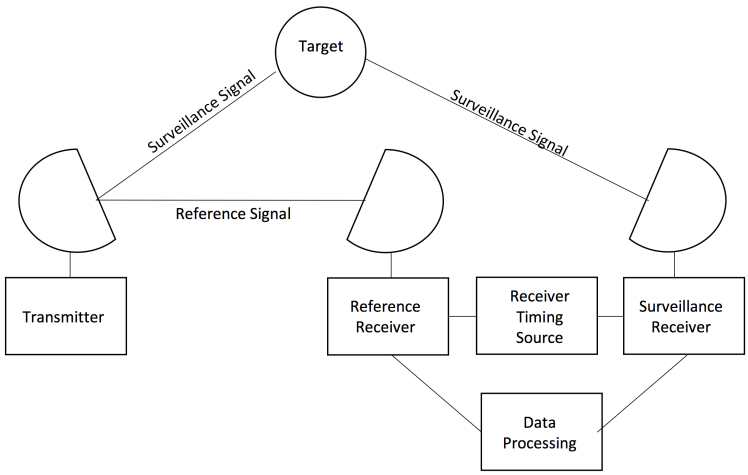


Figure 2.7: Passive Bistatic RADAR Functional Diagram.

The signal path and subsequently range from a transmitter to a target and then on to a receiver is defined as:

$$R = R_T + R_R \tag{2.13}$$

where R is the total signal path length, R_T is the distance from the transmitter to the target and R_R is the distance from the target to the receiver. Figure 2.8 illustrates the two-dimensional bistatic ranging concept, where L is the baseline and β is the bistatic angle. In Figure 2.8 any target that is on the ellipse will result in the same range value of R for a consistent value of L. As outlined previously, additional receivers are required to determine the direction of the target in conjunction with the range.

The PBR equation, as defined by Willis & Griffiths (2007) was developed in two parts; First, the equation is solved for the bistatic maximum range product:

$$R_M = \sqrt{(R_T R_R)_{max}} \tag{2.14}$$

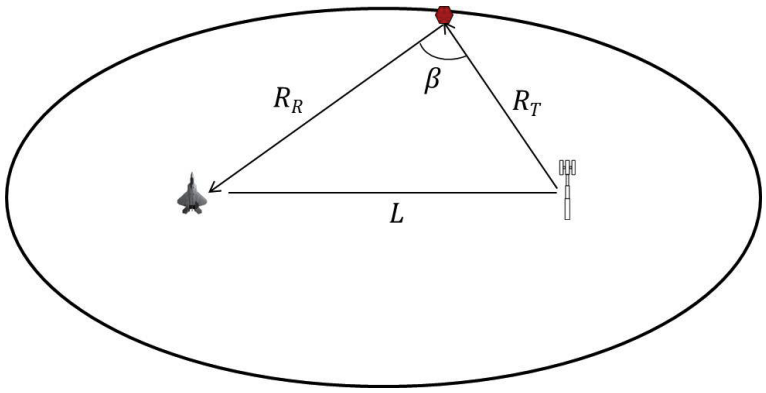


Figure 2.8: Two-dimensional bistatic RADAR geometry (Gutierrez del Arroyo 2012).

Secondly, Cassinian Ovals, a curve defined as the set of points in a plane such that the product of the distances between two fixed points is constant, are plotted with reference to the baseline L to define the geometric properties of the bistatic RADAR equation in terms of a constant Signal to Noise Ratio (SNR). From this, the maximum and minimum ranges and coverage areas can be calculated as a function of R_M.

The PBR range product R_M is equivalent to the monostatic RADAR range calculated in Equation 2.1 and represents the Passive Bistatic RADAR performance as though the receiver and transmitter were co-located. It is therefore useful in comparing the performance of a PBR to a conventional monostatic RADAR. Willis & Griffiths (2007) define the Continuous Wave (CW) form of the bistatic maximum range as:

$$R_M = \left[\frac{P_T \rho G_T G_R t_c \lambda^2 \sigma_B {F_T}^2 {F_R}^2}{(4\pi)^3 k T_i (S/N)_{min} L_T L_R L_{sp}} \right]^{\frac{1}{4}} \tag{2.15}$$

where:

P_T	Transmitter Average Power
ρ	Power Utilisation Factor
G_T	Transmitter Antenna Gain
G_R	Receiver Antenna Gain
t_c	Coherent Processing Interval (CPI) (seconds)
λ	Wavelength (Metres)
σ_B	Bistatic RADAR Cross Section (m^2)
F_T	Pattern Propagation Factor (Transmitter to Target)
F_R	Pattern Propagation Factor (Receiver to Target)
k	Boltzman's Constant ($1.38 \times 10^{-23} J \cdot K^{-1}$)
T_i	Receiver Input Noise Temperature (K)
$(S/N)_{min}$	SNR required for Detection
L_T	Transmitter Losses
L_R	Receiver Losses
L_{sp}	Signal Processing Losses

The pattern propagation factor specified in Equation 2.15 is a term used to describe the wave propagation when free space conditions are not met. This factor is defined separately for the transmitting and receiving paths. The propagation factor also accounts for the RADAR antenna pattern effects (Mahafza 2000). The basic definition of the propagation factor is:

$$F = \left| \frac{E}{E_0} \right| \tag{2.16}$$

where E is the electric field in the medium and E_0 is the free space electric field.

The proportion of the total transmitter power used by the receiver is quantised by the power utilisation factor ρ and is usually accomplished through band limiting. Willis &

Griffiths (2007) also noted that the derived PBR formula makes use of the Coherent Processing Interval (CPI) instead of the more commonly used Noise Bandwidth B_n, as it discourages attempts at achieving overly long detection ranges by reducing the Noise Bandwidth. The CPI is generally limited by the Doppler spread:

$$\Delta f_d = t_c^{-1} = B_n \tag{2.17}$$

If the bistatic angle is significant, the Doppler spread is related to the radial velocity v_r of the bisector $\beta/2$ where Willis & Griffiths (2007) defined the rule of thumb as:

$$\Delta f_d = \sqrt{\frac{v_r}{\lambda}}\ bistatic \tag{2.18}$$

This is half of the equivalent monostatic formula:

$$\Delta f_d = \sqrt{\frac{2v_r}{\lambda}}\ monostatic \tag{2.19}$$

The performance of a bistatic RADAR is reliant upon the specific geometry of the transmitter, target, and receiver. The general bistatic, pseudo-bistatic and forward scattering geometries are illustrated in Figure 2.9.

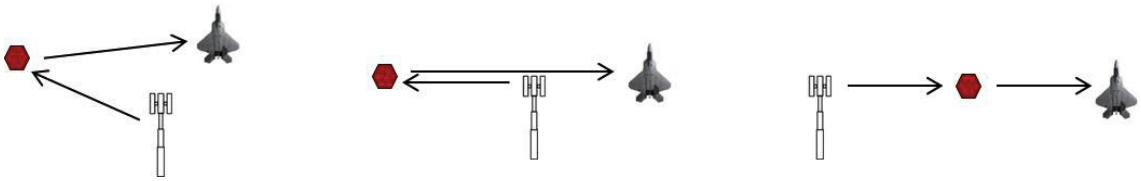


Figure 2.9: Three bistatic geometry cases: *bistatic* (left), *psuedomonostatic* (centre), and *forward scatter* (right). (Gutierrez del Arroyo 2012).

In a configuration where the bistatic angle β is near zero, or where the baseline $L \approx 0$ a bistatic RADAR will operate with a substantial number of monostatic characteristics.

Conversely, where β approaches 180 degrees, the RADAR operation becomes forward scattering, and although cluster scattering coefficients are enhanced, range and Doppler measurements are greatly degraded (Tsao, Weiner, Varshney, Schwarzlander, Slamani & Borek n.d.).

Cassinian Ovals are generally used to illustrate the expected coverage area of a bistatic RADAR based on a modelled detection range. These figures illustrate to a bistatic RADAR designer the expected performance window as a function of the Receiver-Transmitter baseline L. The RADAR Cross Section m^2 (RCS), pattern propagation factors, and receiving noise temperatures are assumed within the coverage areas. Table 2.1 details the range and area calculations for the four general cases as described by Willis & Griffiths (2007).

Condition	**Area**	**Max** R_R	**Min** R_R
$L = 0$	πR_m^2	R_m	R_m
$L < 2R_m$	$\approx \pi \frac{R_m^2 - (L^4)}{(64R_m^2)}$	$\sqrt{R_m^2 + \frac{L^2}{4}} + \frac{L}{2}$	$\sqrt{R_m^2 + \frac{L^2}{4}} - \frac{L}{2}$
$L > 2R_m$	$\approx \pi R_m^2 \frac{R_m^2}{L^2}$	$\frac{L}{2} - \sqrt{\frac{L^2}{4} - R_m^2}$	$\sqrt{R_m^2 + \frac{L^2}{4}} - \frac{L}{2}$
$L \geq 3R_m$	$\approx \pi R_m^2 \frac{R_m^2}{L^2}$	$\approx \frac{R_m^2}{L}$	$\approx \frac{R_m^2}{L}$

Table 2.1: Area and Range calculation for the four constant SNR cases (Willis & Griffiths 2007).

Figures 2.10 and 2.11 show the normalised Cassinian Ovals for the four cases described in Table 2.1. The left focus is the receiver shown always at zero, and the right focus is the transmitter. The contours represent the area of coverage around the transmitter and receiver for a particular baseline of length L. Gutierrez del Arroyo (2012) noted that for $L/R_m \geq 2$ the contour does not show a single oval. Targets located between the ovals are not visible and the RADAR coverage is reduced substantially. The effect is symmetrical with the coverage area over both the transmitter and receiver being equivalent. The separation presented, however, does allow extreme remote sensing applications such as planetary surface observations using either a transmitter or receiver based approach as

detailed by Simpson (1993).

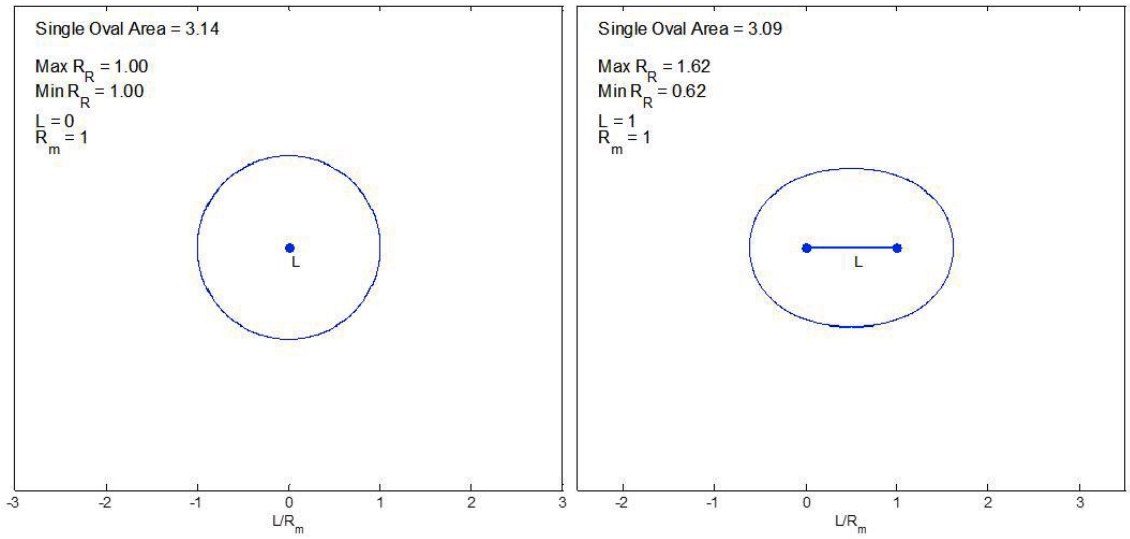


Figure 2.10: Normalised bistatic RADAR range and coverage areas. $L/R_m = 0$ (left), $L/R_m = 1$ (right) (Gutierrez del Arroyo 2012).

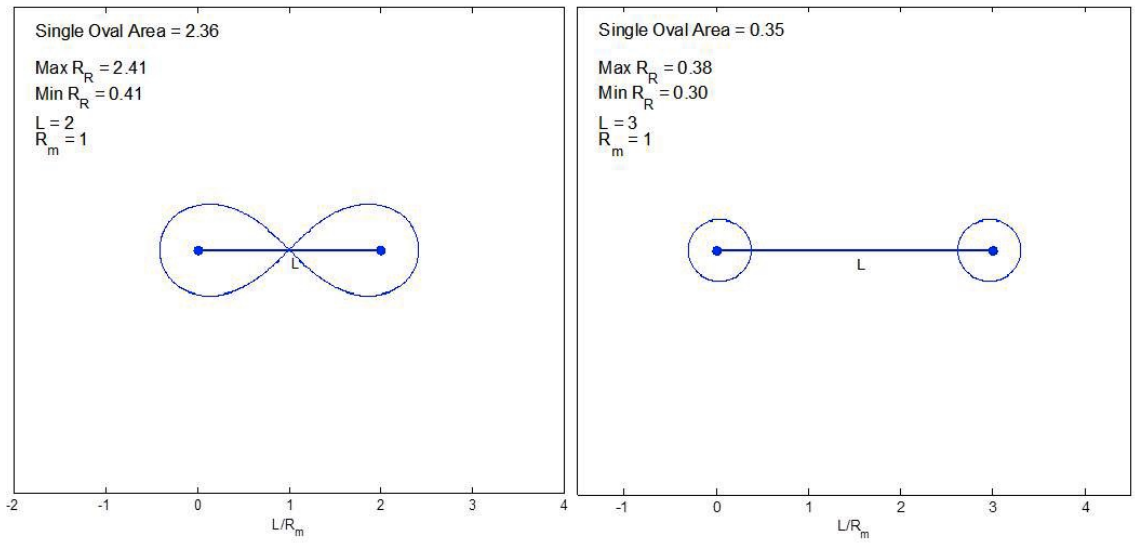


Figure 2.11: Normalised bistatic RADAR range and coverage areas. $L/R_m = 2$ (left), $L/R_m = 3$ (right) (Gutierrez del Arroyo 2012).

For the passive bistatic RADAR transmitters of interest, Bezousek & Schejbal (2008) compiled a table of their typical characteristics, shown at Table 2.2.

Transmitter	ERP (kW)	Range Resolution (km)	Peak Sidelobe Level	
			Range (dB)	Doppler (dB)
FM Radio	50	1.8 → 16.5	-12 → - 27	-26 → - 46.5
DAB+	10	1.5	-11.7	-38
DVB-T	10	0.044	-18.5	-34.6

Table 2.2: Transmitters of Opportunity Signal Characteristics.

2.2.4 The Complex Ambiguity Function

The complex ambiguity function forms the main component of passive bistatic RADAR data interpretation. It is used to acquire insight about the usage of different waveforms in RADAR applications. The Complex Ambiguity Function is a 2D function of time delay and Doppler frequency, and is essentially the output of a matched filter, a commonly used RADAR tool used to match the return signal of a monostatic RADAR to a known range or velocity deviation. Matched filters are often used to reduce processing load, as the filter result can be stored as a constant, reducing the processing cycles required for each data window.

The formula for the Complex Ambiguity Function is given by the correlation of a reference signal with the surveillance signal in both time and frequency, hence a requirement for two independent receivers and antennas, one receiver to collect unaltered data directly from the antenna, and a second to collect surveillance data, containing reflections

from targets. The complex ambiguity function is described as (Ozdemir 2012):

$$X(\tau, f) = \int_{-\infty}^{\infty} s(t)s^*(t-\tau)e^{i2\pi ft}dt \tag{2.20}$$

in the time domain, and subsequently in the frequency domain as:

$$A(\tau, v) = A_{XX}(v, -\tau) = \int_{-\infty}^{\infty} S(f)S^*(f+v)e^{-j2\pi f\tau}df \tag{2.21}$$

where $S(f)$ is the Fourier transform of $s(t)$ being the input signal. The time shift τ represents the delay between the reference and surveillance signal, hence the range of a target can be calculated from this delay. the frequency shift f represents the Doppler shift due to a moving target, or moving receiver, or transmitter, or a combination of all three elements moving at the same time. Where a target is stationary relative to the receiver, the Complex ambiguity function becomes an autocorrelation function of the signal.

The operation and implementation of the Complex Ambiguity Function has been the subject of a number of research papers. The mathematical aspects of the Complex Ambiguity Function were explored by Vandenberg (2012). The implementation of the Complex Ambiguity Function for target detection was explored by Johnson (2001), from which, MATLAB functions for calculating and plotting the result obtained were produced. The functions developed by Johnson (2001) will form the basis of the software implementation used within this research to identify targets from data collected.

2.3 Terrestrial Digital Video Broadcast (DVB-T)

Terrestrial Digital Video Broadcast in Australia conforms to ETSI EN 300 744 V1.6.1, the European digital broadcast standard. The system transmits compressed digital video and digital audio using Coded Orthogonal Frequency Division Multiplexing (OFDM). The operation mode of OFDM is to split digital data into a large number of slower concurrent digital data streams, each of which modulates a set of closely spaced adjacent sub carriers. There are two operational modes that DVB-T can operate under, 2K mode and 8K mode, representing 1,705 or 6,817 subcarriers respectively, that are either 4 kHz or 8 kHz apart. Commonly Australian broadcasters use 7 MHz bandwidth channels, in 8K mode, modulated in 64 Quadrature Amplitude Modulation (QAM).

Generically, OFDM signals carry coded information on multiple subcarriers simultaneously, with the allocated bandwidth being divided equally into N subcarriers, with each being a harmonic of the lowest frequency in the band, ensuring all are mutually orthogonal. The orthogonality allows for close spreading of the data in frequency with minimum interference between them, resulting is a more efficient use of the allocated bandwidth (Gutierrez del Arroyo 2012). The DVB-T standard in 8K mode uses 6,817 subcarriers that are 1 kHz apart.

The use of OFDM in modern digital communications is almost ubiquitous, however, it is seldom used as a non-cooperative RADAR transmitter. This is a result of the complexity of the signal in comparison to an FM source, and the relative infancy of digital modulation technologies in comparison to existing modulation methods that have been present for decades, and are still prevalent worldwide, reducing any requirement to develop PBR receivers for OFDM sources. OFDM RADAR was formally evaluated by Levanon (n.d.) and Levanon & Mozeson (2004), then further developed by Gutierrez del Arroyo (2012).

OFDM waveform generation starts with a randomised set of data bits modulated using Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), or in the case of DVB-T, Quadrature Amplitude Modulation (QAM), producing complex data d_n. When not defined by an international standard or convention as is the case with DVB-T, the signal bandwidth is divided into N subcarriers evenly spaced in frequency by:

$$\Delta f = \frac{B}{N} \tag{2.22}$$

where N is the number of available subcarriers and the discrete Fourier transform length.

The effective signal bandwidth is defined as:

$$B_{eff} = \frac{1}{T_s} = \Delta f \tag{2.23}$$

Gutierrez del Arroyo (2012) found that each n^{th} subcarrier is modulated with the amplitude and phase of a particular dataset d_n, subsequently, all subcarriers are assembled in parallel through an inverse discrete Fourier transform operation then transmitted. The time domain signal becomes a sequence of symbols, each a linear superposition of the N-modulated subcarriers. The communication symbol duration is defined by:

$$T_s = \frac{1}{\Delta f} \tag{2.24}$$

For one (1) communication symbol, the OFDM transmitted signal voltage is modelled in complex form as (Standards Committee 2002):

$$s(t) = e^{j\omega_0 t} \sum_{n=0}^{N-1} d_n e^{jn\Delta\omega t} \ , \ 0 \leq t \leq T_s \tag{2.25}$$

The use of OFDM non-cooperative transmitters has been researched previously by Gutierrez del Arroyo (2012), Levanon (n.d.), and Levanon & Mozeson (2004). The OFDM waveform is also known as a Multi-Carrier Phase-Coded (MPC) signal, and when used as a PBR transmitter, produces a favourable ambiguity function, complex envelope and spectrum when optimised parameters are used. Levanon's (n.d.) general expression for the MPC complex envelope is:

$$g(t) = \sum_{n=1}^{N} \sum_{m=1}^{M} \omega_n a_{n,m} s[t-(m-1)t_b] e^{j2\pi(n-\frac{N+1}{2}\frac{t}{t_b})} \tag{2.26}$$

where ω_n is the nth subcarrier complex weight, $a_{n,m}$ is the mth element of the sequence subcarrier n ($|a_{n,m}| = 1$, and $s(t) \equiv 1$ for $0 \leq t \leq t_b$ and zero elsewhere. The equation describes a sequence of M consecutive symbols, each with their own modulation set ω_n.

2.4 Software Defined Radio

Software Defined Radio (SDR) was born out of the realisation that as the world relies more heavily upon wireless communications, traditional methods relying upon hardware based radio receivers were no longer viable. SDR is a modern implementation of traditional radio hardware. The Wireless Innovation Forum (2014) cites the SDR forum in collaboration with the Institute of Electrical and Electronic Engineers (IEEE) P1900.1 group as having defined SDR as "Radio in which some or all of the physical layer functions are software defined." The definition is extrapolated further to identify that a radio is any wireless device that transmits or receives signals on the Radio Frequency (RF) range of the electromagnetic spectrum, facilitating the transfer of information. The definition encompasses all forms of RF devices from remote controls to complex data links.

A traditional hardware based receiver requires physical changes in order to vary the frequency range over which it can operate (The Wireless Innovation Forum 2014). This limits the functionality of each piece of hardware, and requires either a physical modification for each change, or many individual devices to undertake operation over a wide range of frequencies, using different methods of modulation. A Software Defined Radio (SDR) strips the hardware back to the fundamental elements, and subsequently places all of the remaining hardware into software that produces the same manipulation as hardware through Digital Signal Processing (DSP) (The Wireless Innovation Forum 2014). This flexibility allows multi-mode, multi-band or multi-functional devices that are upgradable by software. Figure 2.12 provides an SDR system overview.

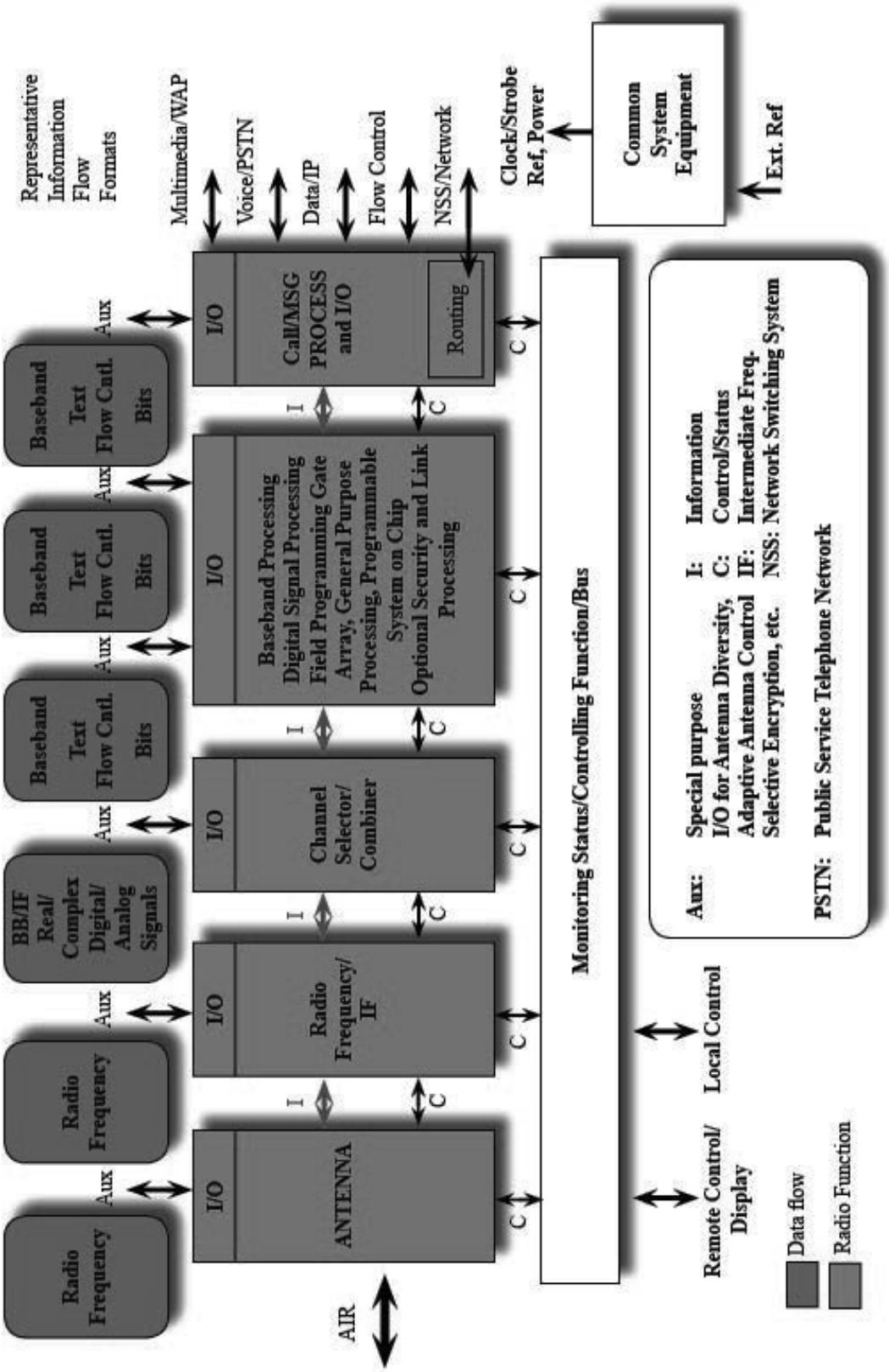


Figure 2.12: SDR Forum Generalised Modular Functional Architecture (Forum 2002).

A Software Defined Radio (SDR) is a collection of hardware and software elements in which some or all of the radio's functions are implemented in software. Some of the common programmable radio elements include:

- Field Programmable Gate Arrays (FPGA);
- Digital Signal Processors (DSP);
- General Purpose Processors (GPP);
- Programmable System on Chip (SoC);
- Other Application Specific Programmable Processors.

2.4.1 Software Defined Radio Software

Software defined radio can be interfaced in a multitude of different methods, the specific interface depends primarily on operating system, and subsequently on the software requirements. For general access to the radio spectrum, SDR# is available for Windows, and GQRX is available for Mac OSX and Linux. Greater flexibility can be introduced in MATLAB or through GNU Radio due to their programability and customisability. There are subsequently a number of task specific applications that have been developed for niche tasks, such as tracking aircraft beacons and receiving trunked radio systems. Each of the hardware drivers can also be accessed directly through programming languages such as python or C#. The most prominent software defined radio applications are detailed below.

2.4.1.1 SDR# Software

SDR# (AirSpy 2016) has become the unofficial standard amongst the software defined radio community, as it is windows based, and provides an unobtrusive graphical user interface, allowing new users to access software defined radio functions without needing to understand any programming language. Originally produced as an open source application, it has since become a closed source (AirSpy 2016). SDR# is based on C++ and is developed for the windows environment, however recent updates have allowed compatibility with Linux and OS X. The primary function of the program is to act as a spectrum analyser, and there are a number of third party plugins that allow greater functionality around the central purpose, however ultimately, the program is limited in what can be achieved.

2.4.1.2 GQRX

GQRX (Csete 2016) is an open source software defined radio receiver. It provides a similar interface to that of SDR# and was originally developed as an alternative that was functional on Linux and Mac OS X systems. GQRX relies on a functional installation of GNU Radio and other dependent applications to operate.

2.4.1.3 MATLAB

MATLAB (Mathworks 2016*a*) is an industry standard for mathematical modelling and testing. MathWorks released an RTL-SDR hardware support package for the communications system toolbox allowing integration of the RTL-SDR hardware to MATLAB

and Simulink (Mathworks 2016*b*). The MATLAB package functions from 22 MHz to 2.2GHz with a sampling frequency range of 225 - 300 kHz or 900 - 2560 kHz. MATLAB interfacing to the RTL-SDR means that all MATLAB functions are able to be carried out on signals received by the RTL-SDR device. The plug-in also provides support for radio addressing, therefore making it suitable for interfacing multiple radio receivers.

2.4.1.4 GNU Radio

GNU Radio (GNURadio 2016*a*) is an open source development toolkit that provides a block based architecture on which software defined radios and signal processing systems can be built. It can function with or without external hardware, to run as a functional radio, or a testing environment. It is based on Python and C++ code, with its open source nature allowing users to add their own blocks, or modify existing blocks as needed for their purpose. The code blocks produced in GNU Radio Companion produce a python script, where all of the program parameters are stored.

2.4.2 Software Defined Radio Hardware

The development of Software designed radio has yielded a number of proprietary and open application hardware devices. Many radio traditional manufacturers such as Uniden, and Kenwood, both radio hardware manufacturers, have developed SDR hardware and software platforms to replace traditional HAM radios and satisfy the amateur radio market, or produced packages for specific professional applications. These implementations are generally closed systems requiring a specific combination of hardware and software to operate within the manufacturer's defined operating range. Proprietary SDR implementations will not be considered within the scope of this research. Conversely,

a number of open hardware platforms have been developed with interface open source SDR software platforms such as SDR# or GNURadio (Wikipedia Contributors 2016). The most common of these hardware platforms as determined by GNURadio (2016*b*) are identified and detailed below.

2.4.2.1 Ettus Research USRP Devices

The Ettus Research Universal Software Radio Peripheral (USRP) range of devices function over an RF range of DC to 6 GHz. The range covers hobbyist through to high bandwidth radios designed for scientific applications. The USRP range of devices have become the unofficial standard for SDR hardware (Ettus Research 2016*a*), and are the platform upon which most existing research on passive RADAR described within this research, has been based. The USRP range of devices range in price from $1,166.00 AUD (2016) to $8,503.00 AUD (2016) with the most common device being the USRP N200, $2689.50 AUD (2016). The primary features of the USRP N210 are outlined in Table 2.3.

Figure 2.13: Ettus Research USRP N200 (Ettus Research 2016*a*).

USRP N200 Specifications	
Use with GNU Radio, LabVIEW and Simulink	2 Gbps Expansion Interface
Modular Architecture: DC-6 GHz	Spartan 3A-DSP 1800 FPGA (N200)
Dual 100 MS/s, 14-bit ADC	1 MB High-Speed SRAM
Dual 400 MS/s, 16-bit DAC	Auxiliary Analog and Digital I/O
DDC/DUC with 25 MHz Resolution	2.5 ppm TCXO Frequency Reference
Up to 50 MS/s Gigabit Ethernet Streaming	0.01 ppm w/ GPSDO Option
Fully-Coherent MIMO Capability	Gigabit Ethernet Interface to Host

Table 2.3: USRP N200 Specifications (Ettus Research 2016*b*).

2.4.2.2 Great Scott Gadgets HackRF

The Great Scott Gadgets HackRF One device functions over an RF range of 1MHz to 6 GHz and was developed as an open source hardware platform, to allow the hobbyist access to SDR. The device has a half duplex transceiver and operates over USB 2.0 unlike the Ettus Research device that operates via Ethernet. This interface presents a disadvantage as it requires the device and processing terminal to be co-located, unlike the USRP devices that can be located with the receive antenna, and away from data processing terminals. The device is powered by the USB bus and therefore requires no external supply. The device is capable of a maximum quadrature sample rate of 20 Msps. Table 2.4 outlines the primary features of the device.

Figure 2.14: Great Scott Gadgets HackRF (Great Scott Gadgets 2016).

HackRF One Specifications	
1 MHz to 6 GHz operating frequency	half-duplex transceiver
up to 20 million samples per second	8-bit quadrature samples (8-bit I and 8-bit Q)
compatible with GNU Radio, SDR#, and more	software-configurable RX and TX gain and baseband filter
software-controlled antenna port power (50 mA at 3.3 V)	SMA female antenna connector
SMA female clock input and output for synchronisation	convenient buttons for programming
internal pin headers for expansion	internal pin headers for expansion
USB-powered	open source hardware

Table 2.4: HackRF One Specifications (Great Scott Gadgets 2016).

2.4.2.3 Nuand BladeRF

The Nuand BladeRF device functions over an RF range of 300 MHz to 3.8 GHz. The device is also capable of operating down to 10 MHz with the use of a block up/down converter, an intermediate device inserted between the antenna and receiver that shifts, by a multiplication factor, the signal presented to it, in order to produce an output that is within the operating range of the software defined radio hardware device. The device is operated over USB 3.0 and is bus powered. The device is capable of full duplex operation and has a maximum quadrature sample rate of 40 Msps. A full list of technical specifications is presented in Table 2.5.

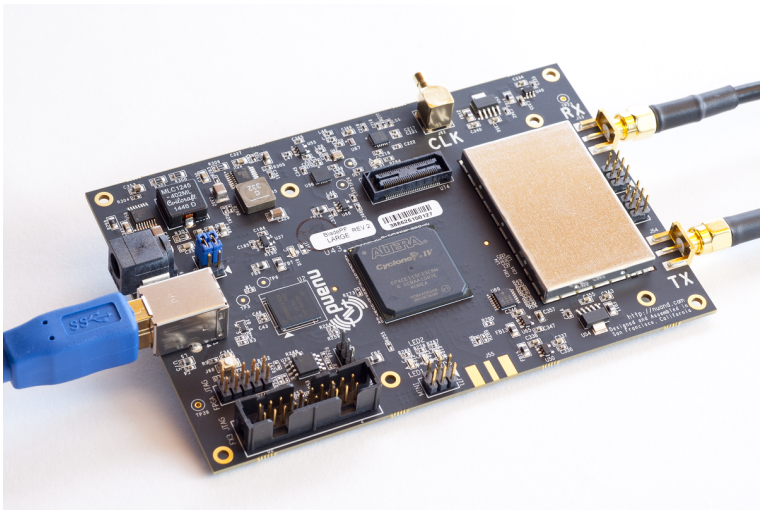


Figure 2.15: Nuand BladeRF (Nuand 2016).

BladeRF Specifications	
Fully bus-powered USB 3.0 SuperSpeed Software Defined Radio	Portable, handheld form factor: 5” by 3.5”
SMA antenna and clock connectors	300MHz - 3.8GHz RF frequency range
Independent RX/TX 12-bit 40MSPS quadrature sampling	Capable of achieving full-duplex 28MHz channels
16-bit DAC factory calibrated 38.4MHz +/-1ppm VCTCXO	On-board 200MHz ARM9 with 512KB embedded SRAM (JTAG port available)
On-board 40KLE or 115KLE Altera Cyclone 4 E FPGA (JTAG port available)	2x2 MIMO configurable with SMB cable, expandable up to 4x4
Modular expansion board design for adding GPIO, Ethernet, and 1PPS sync signal and expanding frequency range, and power limits	DC power jack for running headless
Highly efficient, low noise power architecture	Stable Linux, Windows, Mac and GNU-Radio software support
Hardware capable of operating as a spectrum analyser, vector signal analyser, and vector signal generator	

Table 2.5: BladeRF Specifications (Nuand 2016).

2.4.2.4 RTL-SDR TV Tuners

The RTL-SDR device is based upon the Realtek RTL2832U chipset developed as a TV Tuner, found in a number of USB tuner devices, and televisions. The RTL2832U chipset is an Analogue to Digital Converter (ADC) and Universal Serial Bus (USB) data pump (Osmocom 2016) that is capable of outputting In-Phase (I) and Quadrature (Q) output

data in the same manner as a dedicated SDR receiver, allowing it to be utilised as a SDR receiver. The RF tuning range of the RTL-SDR device ranges from 24 MHz to 2200 MHz, although this does vary based upon the tuner chip used, Table 2.6 outlines the tuning range based upon the tuner chipset used.

RTL-SDR Tuner Ranges	
Tuner	**Frequency Range**
Elonics E4000	52 - 2200 MHz with a gap from 1100 MHz to 1250 MHz (varies)
Rafael Micro R820T	24 - 1766 MHz
Rafael Micro R828D	24 - 1766 MHz
Fitipower FC0013	22 - 1100 MHz (FC0013B/C, FC0013G has a separate L-band input, which is unconnected on most sticks)
Fitipower FC0012	22 - 948.6 MHz
FCI FC2580	146 - 308 MHz and 438 - 924 MHz (gap in between)

Table 2.6: RTL-SDR Tuner Ranges (Osmocom 2016).

The additional functionality of the RTL2832U chipset was discovered by Antti Palosaari (Cass 2013) and further developed by Osmocom to produce functional driver sets. Devices containing the RTL2832U chipset are commonly available in online stores for under $20.00 AUD (2016) and provide an affordable device for SDR (Osmocom 2016). Unlike the purpose designed SDR dongles, the RTL-SDR provides only an 8-bit quadrature Digital to Analogue Converter (DAC), substantially reducing its bandwidth. The theoretical maximum sampling rate of the RTL-SDR is 3.2 Msps, however anecdotal testing evidence suggests a practical maximum closer to 2.56 Msps (Osmocom 2016).

The disparity between the identified bandwidth of 2.56 Msps and the 7 MHz bandwidth of a DVB-T channel can be accounted for in the processing method used. Osmocom (2016) has identified that DVB-T processing occurs internally within the RTL2832U chip, with the demodulated data passed over USB, conversely, when the dongle is imple-

mented for SDR the in-phase and quadrature data is passed without any processing at the limited bandwidth of 2.56 MHz, hence the dongle's ability to process DVB-T signals is severely impaired.

The clock used on the RTL-SDR is a 28.8 MHz crystal oscillator, some hardware developers are producing devices with a Temperature Controlled Crystal Oscillator (TCXO), which have a high quality, or Q factor, representing a low rate of energy loss and a higher quality oscillation. The high quality TCXO components used present limitations with regard to the project scope as they are substantially more expensive than the standard dongles (RTL-SDR.com 2016*a*). Table 2.7 outlines the product specifications of the RTL-SDR dongles.

Figure 2.16: Typical RTL2832U Based TV Tuner.

RTL-SDR Specifications	
Bus Powered USB 2.0	24 - 1766 MHz Frequency Range
8-Bit I/Q DAC	Maximum 3.2 Msps Sampling Rate
Actual 2.56 Msps Sampling Rate	

Table 2.7: RTL-SDR Specifications (Osmocom 2016).

2.4.3 Coherent Clock Hardware

Receiving a Passive Bistatic RADAR (PBR) signal requires multiple hardware receivers to capture an unobstructed reference signal from the transmitter, and a reflected surveillance signal from the target. Each of the receivers in use then requires a coherent clock source to provide a timing reference to the received data. The hardware structure for a PBR is shown in Figure 2.7. There are a number of clock generators available from Hewlett-Packard and Tektronix, however, they are extremely expensive and only available in a laboratory environment. Alternatives that were cost appropriate are considered below. The standard circuit diagram of the RTL-SDR clock configuration is shown in Figure 2.17

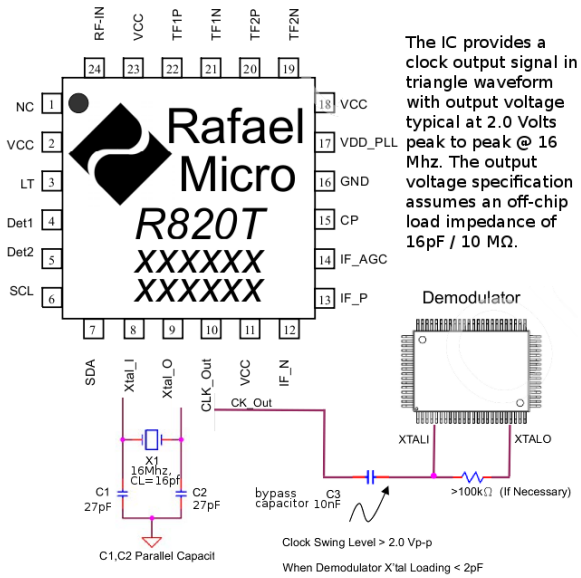


Figure 2.17: RTL-SDR Clock Configuration (Superkuh 2016).

.

2.4.3.1 Passive Clock Sharing

Whilst the clock on an RTL-SDR board will vary with temperature quite considerably (Hyde 2015), essentially, so long as the variation between multiple dongles is coherent, the results of any experiment involving multiple signal sources should be valid. To this effect, Salsburg (2015) extended the clock signal from one RTL2832U based dongle to a second, with a third dongle from a single clock being identified as the maximum load. The implementation is shown in Figure 2.18. Salsburg (2015) has identified that to undertake this implementation, it was necessary to remove the crystal and both capacitors on the slave dongles. The coherent dongles must then be linked together using a coaxial cable. Installing an RF capacitor on the source dongle output to eliminate the loading effect while still passing the clock signal is also necessary. Passive clock sharing presents limitations to the functionality of a PBR as the oscillation of crystal occasionally exceeds the operational limits of the RTL2832U chipset, resulting in packet loss. Where signal coherence is required between multiple dongles, any packet loss will alter the long term coherence of the system, and result in data processing errors. Based upon the results presented in Section 5.3, it was determined that passive clock sharing was not a suitable option for achieving clock coherence between multiple dongles.

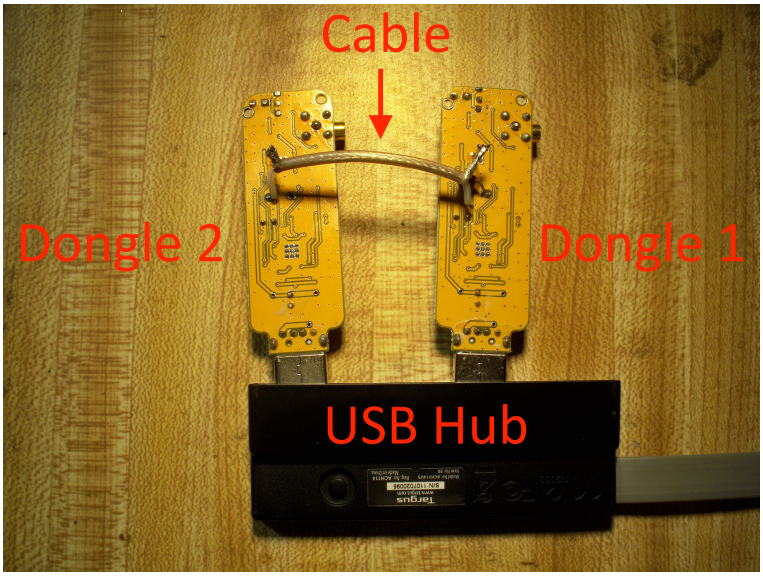


Figure 2.18: Two RTL-SDR Dongles sharing a single clock source (Salsburg 2015).

.

2.4.3.2 Texas Instruments CDCLVC1310-EVM Evaluation Board

The Texas Instruments CDCLVC1310-EVM Evaluation Board was developed for experimentation based around the CDCLVC1310 IC. The evaluation board comprises of the Integrated Circuit (IC), an internal 25 MHz clock source, an internal clock source, and 10 low jitter, low power clock outputs (Texas Instruments 2011). The implementation of the Texas Instruments CDCLVC1310 Evaluation board was proposed by a Romanian tester who only provides reference to himself by amateur radio callsign, YO3IIU (2014), who replaced the supplied 25 MHz onboard crystal oscillator with a 28.8 MHz TCXO to produce an accurate reference of approximately 2.5ppm. Configuration of the RTL-SDR dongles required the removal of the existing crystal oscillator and associated capacitors, and a coaxial cable installed in place of the crystal oscillator. Testing of the evaluation board with four RTL-SDR dongles connected indicated that the clock drift between oscillators was no longer extant, however, due to the nature of USB acquisition and data

processing, it was noted within YO3IIU's (2014) research, that there was still a slight variance that needed to be removed in software.

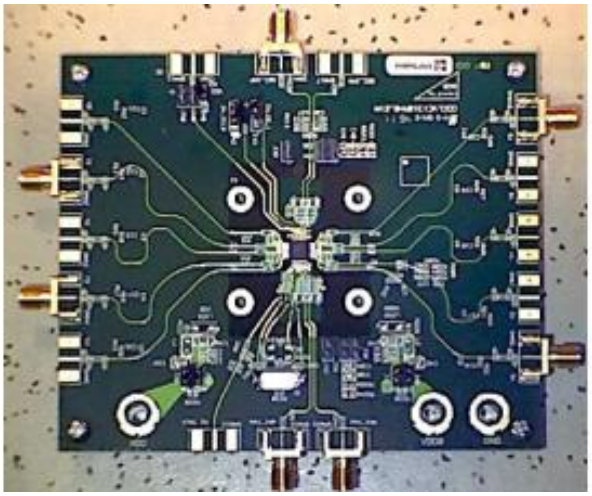


Figure 2.19: Texas Instruments CDCLVC1310 Evaluation Module (Texas Instruments 2016).

.

2.4.3.3 Arduino Based Si5351a Voltage Controlled Oscillator

It was identified by van de Swaluw (2015) that a viable alternative to the Texas Instruments CDCLVC1310-EVM Evaluation board discussed at 2.4.3.2 exists. The Si5351A Voltage Controlled Oscillator (VCO) is an I^2C configurable clock generator that provides 3 clock outputs between 8 kHz and 160 MHz with an approximate 0ppm error. This accuracy is achieved through the use of a phase locked loop (PLL), whereby a feedback loop is used to determine and subsequently correct any deviation from the intended output frequency. Another benefit of the Arduino based solution is that the library developed by Milldrum (2016) enables the output clock power to be regulated, hence, the internal noise generated in the circuit at multiples of the clock frequency can be substantially reduced. Configuration of the clock generator is achieved through an

Arduino sketch, which, once loaded will operate independently of a computer interface. Similarly to other methods, the configuration of the RTL-SDR dongle requires removal of the existing crystal oscillator and associated capacitors shown in Figure 2.17. The clock signal is injected via high pass filter making use of a 10 nF and a 28Ω resistor, providing an impedance match to the clock generator output. The Adafruit (2016) Arduino breakout board is shown in Figure 2.20

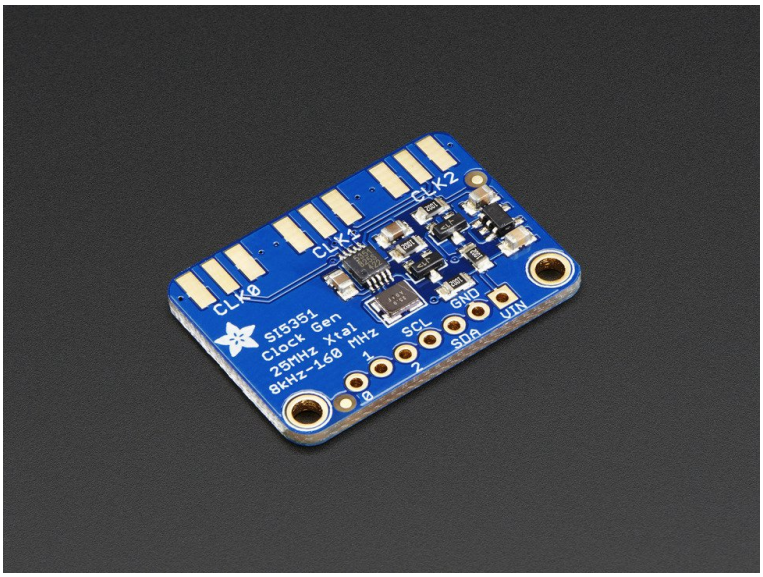


Figure 2.20: Texas Instruments CDCLVC1310 Evaluation Module (Adafruit 2016).

.

2.5 Literature Review

This section provides a comprehensive literature review on the implementation of passive RADAR through software defined radio, the use of DVB-T signals to produce an ISAR output and the Realtek RTL2832U TV tuner as an SDR reeiver.

2.5.1 Frequency Modulated Continuous Wave Passive RADAR

Frequency Modulated Continuous Wave (FMCW) passive bistatic RADAR makes use of non-cooperative commercial FM radio broadcasts to acquire a target. The target range and speed are resultants of this type of passive RADAR. The RADAR is also able to resolve the arrival or departure of the target.

The Thales Homeland Alerter 100 (Group 2010) and Lockheed Martin Silent Sentry (Freeman 2007) are examples of commercially developed passive RADAR systems that rely upon analogue FM broadcasts to detect and track aircraft over large geographical areas.

It was identified by Bezousek & Schejbal (2008) that the nature of a typical FM broadcast signal means that the *bandwidth fluctuates depending upon the content being broadcast.* A typical pop song will produce a suitable result, with heavy metal being favourable (Stevens 1988), however speech leads to pauses and inconsistencies in the frequency domain. Digital Audio Broadcasts were identified as a potentially better alternative.

It was identified by Franklin (2010) that the difference in modulation index of an FM broadcast was based on the input type. The work shows results for classical music, rock music, jazz music, and speech. The modulation index varies markedly dependent upon the type of input. The results of this analysis can be seen in Figure 2.21.

Szlachetko & Lewandowski (2012) proposed an implementation of FM passive bistatic RADAR making use of GNU Radio and the USRP2 with hardware modifications for multiple coherence receive channels. The implementation of multiple channels allows for triangulation of the target based on the phase changes between transmitters at known locations. As described in Section 2.2.3 the overlapping range equation results confer to provide a location of the target. Similarly, Heunis, Paichard & Inggs (n.d.) developed a

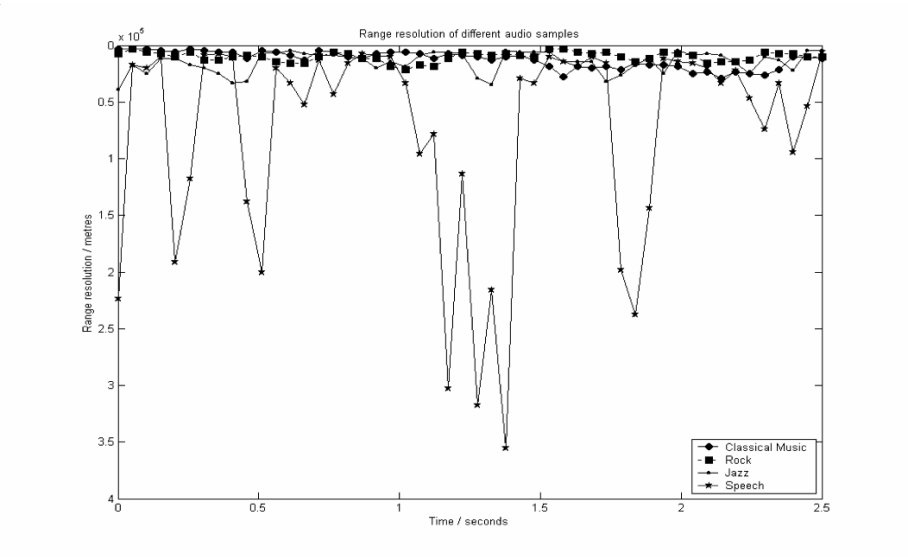


Figure 2.21: Range Resolution of FM Modulated Audio Signals (Franklin 2010).

successful implementation of a passive bistatic RADAR utilising GNU Radio and USRP hardware.

In the absence of a viable alternative, Analogue FM transmissions make a suitable passive RADAR transmitter source. Its use is constricted by the variations in modulation frequency, meaning that it cannot be relied upon. The recent progressions in technology identified in Section 2.5.2 provide a more reliable signal source that is independent of the broadcast content, and therefore a more reliable alternative when implementing a passive bistatic RADAR.

2.5.2 Orthogonal Frequency Division Multiplexed Passive RADAR

OFDM passive bistatic RADAR makes use of spread spectrum digital signals to track targets. Unlike analogue signals, an OFDM signal exists consistently regardless of the content being transmitted. This stability enables it to be used more reliably as a non-cooperative transmitter for passive RADAR. Examples of OFDM signals that are easily

identified include mobile telephone transmitters, digital audio broadcast radio, digital television transmitters, WiMax, and Wi-Fi.

Tigrek (2010) proposed and simulated a method of using an orthogonal frequency division multiplexed communications signal to transceive data between two locations and concurrently interpret passive bistatic RADAR data from the same signal. The modelling makes use of a full understanding of the transmitted signal to deconstruct the reflected return path. It is identified within the text that OFDM signals by their nature provide a greater Doppler sensitivity.

Petri, Berizzi, Martorella, Mese & Capria (n.d.) developed an experimental test whereby they make use of the Universal Mobile Telecommunications System (UMTS), which functions on an OFDM architecture to firstly verify the signal source as a valid non-cooperative transmitter, and subsequently to detect and track targets. Their work shows valid experimental results.

Olivadese, Giusti, Petri, Martorella, Capria, Berizzi & Soleti (n.d.) demonstrated a passive inverse synthetic aperture RADAR using a DVB-T signal as the source. The implementation uses Ettus Research USRP hardware and MATLAB for software processing. The results achieved show an unfocussed two dimensional image of an intended target, with data acquired from three (3) adjacent DVB-T transmitter channels.

The bandwidth, periodicity and composition of OFDM signals make them an attractive method of implementing passive bistatic RADAR. The constant nature of the signal and recurrant preamble reduce the error that is introduced by traditional FM broadcast signals. Based on the literature reviewed, it is not anticipated that the full scope of OFDM interpretation will be required in order to achieve the objectives of this project.

2.5.3 RTL2832U based Passive RADAR

McKay-Bukowski, Vierinen, Virtanen, Fallows, Postila, Ulich, Wucknitz, Brentjens, Ebbendorf, Enell, Gerbers, Grit, Gruppen, Kero, Iinatti, Lehtinen, Meulman, Norden, Orisp, Raita, Reijer, Roininen, Schoenmakers, Stuurwold & Turunen (2015) are recognised as being the first to attempt the implementation of a passive bistatic RADAR based on RTL-SDR hardware. The implementation requires a minimum of two dongles, and hardware modifications to achieve a coherent timing clock. An algorithm is subsequently required to eliminate the incoherence introduced by the operation of the USB protocol.

The implementation of passive bistatic RADAR developed by McKay-Bukowski et al. (2015) has a number of limitations. The timing source shown in Figure 2.7 is reliant upon the existing crystal oscillator, which is not stable and is temperature sensitive. The clock distribution is also passive, this introduces additional loading on the crystal oscillator, further reducing the reliability of the hardware configuration. Whilst the clock variation is not critical, so long as both dongles receive the same data, an external clock source would produce a more reliable result. The software implementation has been developed in Python, which limits expansion of the code, primarily due to the speed at which Python developed implementations execute. As a result, it is unlikely that a Python based implementation could operate in real time.

Salsburg (2015) produced an RTL-SDR based receiver with a passive coherent clock, however there is no data presented to show the effective implementation of a passive bistatic RADAR based on the hardware.

Leech (2013) and Schrödle (2014) developed implementations of the RTL-SDR dongle using external timing sources including the use of function generators such as the Hewlett Packard HPAK 8662A with a timing accuracy better than 0.0005 ppm, per day and GPS

based clock devices.

It was identified by van de Swaluw (2015) that it was not necessary to use a function generator as an external timing source for coherent RTL-SDR dongles, and that an Arduino with a Silicon Instruments Si5351A based shield could be used to produce the requisite 28.8 MHz clock and achieve a 0 ppm shift. Similarly, YO3IIU (2014) made use of a Texas Instruments TI CDCLVC1310-EVM Evaluation board, with the supplied 25 MHz crystal oscillator replaced by a 28.8 MHz temperature controlled crystal oscillator to provide 10 stable clock outputs, allowing the connection of multiple dongles, and placing the physical limitation onto the USB hardware and serial data transfer.

Silverwood (2014) uploaded a video to YouTube depicting an implementation of the same passive RADAR method implemented by McKay-Bukowski et al. (2015) above, however the implementation makes use of Sydney, NSW digital radio multiplex channel 9A on 202.928 MHz. This implementation had minimal pre-processing, only making use of the complex ambiguity function described in Section 2.2.3. Data processing for this implementation was undertaken in MATLAB.

Due to the lack of peer-reviewed, journal published articles, the data produced by prior researchers is anecdotal. The work undertaken to date focussed primarily on analogue FM radio transmitters, and where a passive bistatic RADAR has been implemented, the modifications made to the RTL-SDR hardware do not use an accurate timing source. Additionally, the supplied evidence suggests that interfacing was directly written in Python and does not make use of the unofficial standard GNU Radio, nor the universally accepted MATLAB. The implementation of external timing sources is a valid way of implementing coherence and will be explored in greater depth in the dissertation. Further research is required into the use of RTL2832U based receivers as a passive bistatic RADAR.

2.5.4 Chapter Summary

This chapter has presented existing research and data in the area of passive bistatic RADAR, it has presented a range of systems, the current implementation methods, an explanation of the transmitter sources for passive bistatic RADAR, and a detailed explanation of the hardware and software available to conduct further research. A literature review was conducted on the different types of waveform that are suitable for use as a passive bistatic RADAR source, and existing work presented. A literature review was also conducted on previous work conducted with RTL-SDR hardware as a passive bistatic RADAR receiver, identifying opportunities for further research to be conducted.

3

Methodology

This chapter presents the methodology used to determine the suitability of the Realtek RTL2832U chipset based receiver as a Passive Bistatic RADAR (PBR) front end, the testing methodology and verification methodology.

3.1 Introduction

A design methodology based upon the classical engineering approach was employed in the undertaking of this research. This method of research involved the determination of an implementation method, followed by testing and continual refinement to determine the most viable solution to the project requirements. The primary objective of the project, identified within the project specification was a low cost implementation making use of Software Defined Radio (SDR).

Based on the project objective, it was determined that the passive bistatic RADAR implementation would have the requirements of a feature set including:

- a low development cost of less than $100 AUD (2016) for each receiver;
- processing based on a Software Defined Radio (SDR) solution; and
- hardware receivers based on TV tuners using the RTL2832U chipset.

Existing research into passive RADAR involved the use of proprietary systems, such as those developed by Thales (Group 2010), and Lockheed Martin (Freeman 2007), or a reliance on the Ettus Research USRP (Ettus Research 2016*a*) series of receivers. Each of these existing implementations required a substantial financial investment to receive radio signals that were already present, and received on devices that were much lower in cost. The Defence Science and Technology Group (DSTG) undertook research into PBR with a hardware cost of approximately $60,000 AUD (2014) (Palmer 2014). Independent to any hardware receiver, where much of the system cost is borne, the processing method used for a PBR would remain effectively the same. Based on this conclusion, it was determined that a low cost PBR implementation would contribute valid research to the field, that could be translated through any applicable hardware

platform, based on the scale requirements of the user.

Traditionally, RADAR was implemented through discrete components to produce matched filters and undertake signal processing. With technological progression, commercial RADAR manufacturers developed proprietary hardware and software based RADAR decoders. These proprietary systems are not available to developers, and hence cannot be used as a basis for development of a passive RADAR system. Given the substantial limitations imposed by the use of a discrete component implementation, it was determined that Software Defined Radio (SDR) was the most appropriate method for PBR processing development, a further benefit achieved by the SDR processing method was hardware scalability based on system requirements, without the need to redevelop the entire system.

As SDR was determined the most viable PBR processing method, a compatible hardware receiver was required. Of the SDR receivers identified in Section 2.4.2, it was determined that the Ettus Research USRP device was the most viable for use, providing the most comprehensive feature set, and the greatest probability of implementation success. The Ettus device, however, was considered expensive, and did not meet the project requirement for a low cost implementation, as such, it was discounted as a viable solution. The Great Scott Hack RF One and Nuand Blade RF were secondary considerations for use, however both devices still exceeded the low cost requirement of the project. RTL2832U based TV tuners were ultimately chosen as a suitable device for development of a PBR as they were capable of receiving signals within the required frequency range, and only require minimal modification to be used. It was determined that the cost of the device, and modification was substantially lower than the cost of any alternate hardware SDR receiver.

The literature review determined that there is substantial previous research into bistatic passive RADAR implementation with a non-cooperative FM source, and anecdotal evidence to support it having been implemented on an RTL-SDR platform. Based on

the scarcity of literature to support an implementation of bistatic passive RADAR using RTL-SDR hardware and a commercial television broadcast as the non-cooperative transmitter, it was determined that further work was required in this area of the field. The methodology presented within this chapter has been developed to achieve the research objectives outlined in Section 1.4.

Continuous wave, Frequency Modulated Continuous Wave, and Synthetic Aperture RADAR properties were investigated to determine the most useful type of passive bistatic RADAR. It was necessary to understand the different RADAR definitions, their interactions and subsequently their applications in order to determine the usability of each type based on the hardware available, for this application, that was RTL2832U based dongles.

The required hardware design modifications of a RTL-SDR dongle were investigated and tested to optimise the hardware operation for the lowest cost. Once the basic operation of the hardware was confirmed, a PBR was simulated with a doppler RADAR configuration to ensure the hardware function was suitable. Subsequent testing was then carried out with a frequency modulated continuous wave, and then an OFDM wave, being that of a Digital Television Broadcast (DVB-T) signal.

The configured hardware and software underwent testing in different environments to evaluate its suitability. The results of these tests were evaluated in relation to the:

- suitability of RTL2832U based TV Tuners as PBR receivers;
- suitability of the integrated software platform for producing a RADAR display;
- functionality of the hardware in a simulated environment;
- functionality of the hardware using a non-cooperative transmitter; and
- suitability of the hardware as an inverse synthetic aperture RADAR receiver.

Sufficient time, would have enabled additional work to be undertaken to determine the requirements and subsequently implement a direction finding capability into the RADAR receiver based upon a known North reference point. Due to the results achieved, and the limitations surrounding data collection sites, it was not possible to undertake the additional work required to implement a direction finding capability into the passive bistatic RADAR.

3.2 Hardware

A set of hardware devices was developed to determine the suitability of RTL-SDR dongles as bistatic passive RADAR receivers. The hardware configuration was based upon an external timing signal generator and two RTL-SDR receivers. Additional hardware was developed to verify the functionality of the RTL-SDR based device. Figure 3.1 shows a block diagram of the proposed hardware configuration for testing.

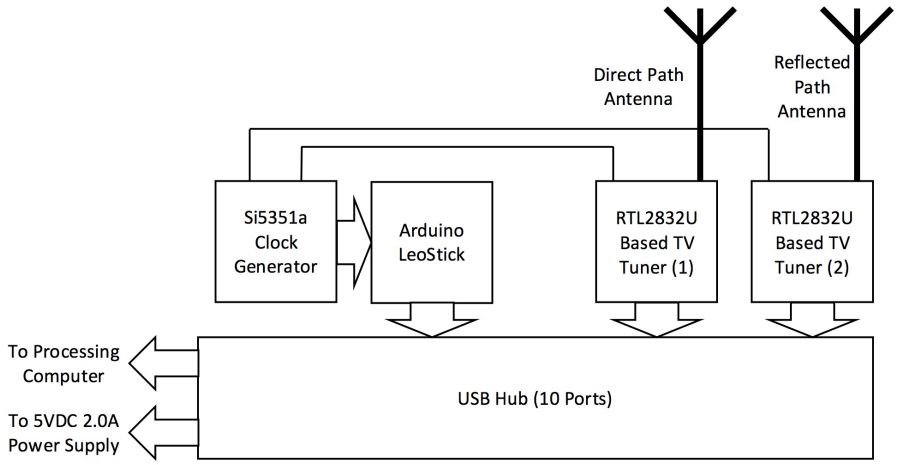


Figure 3.1: Proposed Hardware Block Diagram of SDR Passive RADAR Implementation.

3.2.1 Bistatic Passive RADAR Receiver Device Configuration

A hardware configuration based upon two RTL-SDR receivers was constructed, with modifications undertaken to remove the internal clock, and modify the extant antenna connection. The literature review in Section 2.4.3 identified that the internal clock source provided with RTL-SDR receivers was inadequate for a coherent multi-receiver configuration, hence it was removed, and modified to provide an SMA connector for interfacing to an external clock source, based upon the work in Section 2.4.3.3.

The existing antenna connection on the dongle was modified to provide SMA connectors at the rear of the metal enclosure. This provides a standardised fitting and ensures easy accessibility to connect antenna sources to the device. As a way of minimising errors introduced by the USB input, both dongles shared a single USB hub and made a single connection to the testing computer hardware.

3.2.2 External Timing Signal

Based upon the findings of Section 2.5, it was determined that an Arduino based VCO utilising an Si5351 breakout board, was the most suitable source for providing an external timing signal to the RTL-SDR dongles, and subsequently, enable the collection of passive bistatic RADAR data. The external timing source was to be tested to confirm that the output is more accurate and stable than the result provided by the internal RTL-SDR clock. An accurate and stable timing signal ensures coherence between the two receivers used, and ensures operation within the functional limits of the RTL2832U chipset is maintained to prevent packet loss. Results from the external clock validation are located in Section 5.4.

The validated clock signal was to be used as an input to the multiple dongles required to collect passive bistatic RADAR data. A suitable program based on the Arduino Si5351 Library (Adafruit 2016) was to be developed to produce a 28.8 MHz clock signal, commensurate to the timing source provided by the original internal crystal oscillator.

3.2.3 Reference Receiver

To validate any passive bistatic RADAR target acquired through the developed hardware and software, it was necessary to have an alternative location identifier. Based upon this requirement, it was determined that aircraft would provide the most accessible target source, and they could be verified by the on board locator beacon.

All commercial aircraft in the region of interest are fitted with an Automatic Dependent Surveillance - Broadcast (ADS-B) transponder. The transponder provides details of the aircraft location as a latitude and longitude, details of the aircraft altitude, and details of the aircraft velocity (Air Services Australia 2016). The data from the aircraft is broadcast at 1090 MHz and is transmitted at a range greater than 250 nautical miles.

Based upon the functionality provided by ADS-B, a hardware and software configuration was developed to verify the location of aircraft intended to act as passive bistatic RADAR targets to confirm the operation of RTL-SDR receivers for passive bistatic RADAR. The results of this verification are presented along side the results of RTL-SDR passive bistatic RADAR data collection in Sections 5.11 to 5.13.

3.2.4 Continuous Wave Generator

To verify the operation of the RTL-SDR based passive bistatic RADAR receiver, a continuous wave transmitter was to be developed. The transmitter was to be capable of producing a controlled output, suitable to be received by the PBR receiver and processed to produce a valid Doppler output, from which the velocity of object within the surveillance signal path can be calculated. The results of the testing conducted with the continuous wave generator are presented in Section 5.9.

3.3 Software

Software implementation was primarily undertaken in MATLAB, making use of the work previously conducted by Johnson (2001) with the complex ambiguity function to process data. The overall software function was to:

- read direct path and reflected path signal;
- filter direct path signal;
- mix direct path and reflected signal;
- process the signal difference to identify targets; and
- produce waterfall diagram to display identified targets.

A linux environment and GNU radio were also used to collect coherent data samples based upon the work carried out by Krysik (2016). Additional work was carried out with GNU Radio to produce a software only doppler RADAR, capable of verifying the

functionality of the MATLAB implementation.

3.4 Testing

A range of testing was conducted to verify the operation of individual components within the system, and subsequently, the operation of the completed hardware configuration.

3.4.1 Internal Timing Clock Examination

To validate the work presented in Section 2.4.3, it was necessary to undertake testing on the internal RTL-SDR dongle crystal oscillator. To determine the stability of the clock, it was to have the timing components connected at room temperature to an oscilloscope, the oscilloscope was to be configured to log the frequency of the oscillator at 1 second intervals for a period of 1 hour, in order to gather a sufficient sample set to determine oscillator function.

As logging commenced, the dongle was to be connected to a computer, and tuned through an appropriate SDR application to receive data throughout the test. This configuration would provide sufficient load that the dongle would rise to its regular operating temperature of approximately 40°. The results of this internal clock examination are presented in Section 5.3.

3.4.2 External Timing Clock Verification

Hardware testing occurred through verification of the coherent timing source on an oscilloscope. The Arduino based timing source was connected to the oscilloscope and data logged over a period of 1 hour at 1 second intervals to measure and confirm any drift from the intended 28.8 MHz clock speed.

As logging commenced, the dongle was to be connected to a computer, and tuned through an appropriate SDR application to receive data throughout the test. This configuration would provide sufficient load that the dongle would rise to its regular operating temperature of approximately 40°. The results of this internal clock examination are presented in Section 5.4.

3.4.3 RTL-SDR Dongle Testing

Initial validation testing was to occur by confirmation that the dongle operated in the same manner as it had prior to modification. This was proven by connecting the dongle individually to both the external timing source, and to a computer, and tuning to a receivable frequency. GQRX (Csete 2016) is capable of decoding AM and FM signals, so it was beneficial to tune the receiver to a radio frequency that was easily decoded. Each dongle's response to the tuned frequency was to be recorded and compared. With all dongles producing equivalent results, it can be concluded that the modification had not caused any change in operation. If any results did not concur, that dongle would be deemed faulty and not suitable for use in a passive bistatic RADAR receiver configuration.

For each development stage occurred in a controlled environment making use of fre-

quencies within the ISM band operating within prescribed power levels to ensure safety. Testing of the hardware was conducted over several types of RADAR modulation to verify the functionality of the hardware prior to undertaking testing with non-cooperative transmission sources.

The overall performance of each dongle also required testing. Determining the noise floor of each dongle required a dummy load to be connected, and a long duration scan conducted over the receivers full range. Any internal noise within the dongle, and hence, the dongle noise floor will be visible in the results. The results from this testing are presented in Section 5.6.

3.4.4 RTL-SDR Dongle Calibration

As the Si5351 oscillator still makes use of a crystal oscillator, there will still be an offset from 28.8 MHz present. In order to account for the inherent offset within the crystal, it must be calibrated. Calibration requires a consistent signal source to determine the offset. Conveniently, the Global System for Mobile Communication (GSM) mobile telephone system provides a solution.

Mobile telephone timing sources function in a similar way to the unmodified RTL-SDR dongle, with a basic crystal oscillator, and subsequently an offset from the intended clock frequency that is variable, dependent upon the operating conditions. The follow-on effect of the timing signal variance is a drift in the uplink and downlink frequencies between the phone, and the standardised frequency expected, and provided, by the cell tower. To overcome this drift, GSM implements a frequency correction channel, which transmits a 67.7 kHz tone from the base station to a mobile phone. By calculating the difference between the actual tone received, and the known reference of 67.7 kHz, it is possible to determine the clock source offset (Markgraf 2012).

This functionality was exploited to determine the offset of the Arduino based Si5351 external timing source generator. Markgraf (2012) has developed a program to utilise this calibration method with RTL-SDR dongles. The results of the calibration are presented in Section 4.10.

3.4.5 Passive RADAR Data Collection

Data collection to determine the suitability of an RTL-SDR based passive bistatic RADAR occurred over a number of steps, to verify the operation of the developed MATLAB program, software based testing must occur. The testing was required to provide a continuous wave doppler reference and surveillance signal, from which the MATLAB program could extrapolate doppler shift. The results of this testing determined whether the software implementation was viable. Results of this testing are presented in Section 5.8.

With a confirmed software implementation, the next data collection stage was to implement a hardware validation test. Making use of the same signal type, a continuous wave transmission, a sufficient separation was to be used to transmit the signal, and receive it on two RTL-SDR dongles. Movement was to occur within the field on one receiver, then the result processed through the MATLAB program. The results of this testing provided confirmation that RTL-SDR dongles are capable of functioning as passive bistatic RADAR receivers. The results from this test are presented in Section 5.9.

A suitable location from which passive bistatic RADAR data from a range of non-cooperative sources could be acquired was to be determined. The location was required to be within suitable distance of transmitter sources, and within a reasonable range of targets, in order to produce definitive results. The determined location was to have band scans conducted over the frequencies of interest to confirm suitability. Results from the band scans are presented in Section 5.7. Where possible, the DVB-T functionality of

the RTL-SDR dongles was to be used to collect data on the available DVB-T sources visible from the data collection location. The results of the data collection location determination are located at Section 5.10.

Final testing occurred initially with a verification of the hardware by testing against an FMCW source such as a commercial FM radio station. This verified the operation of the hardware in real world environments. Subsequently, testing was conducted on a commercial DAB+ transmitter, and subsequently a commercial television transmitter source to determine the suitability of the hardware as a passive bistatic RADAR receiver for transmitters using OFDM. The results obtained from this testing are presented in Sections 5.11, 5.12, and 5.13 respectively.

The results of the testing were contrasted against the requirements of an inverse synthetic aperture RADAR and modelling conducted to determine whether data acquired by the hardware will produce an inverse synthetic aperture RADAR output.

3.5 Chapter Summary

This Chapter has presented an explanation of the methodology required to validate the project objectives described at Section 1.4. The chapter has described the hardware, software and testing procedures required, and has explained the process undertaken to achieve a result. This chapter also presented a system diagram, from which the methodology was developed. The design undertaken based upon the methodology in this Chapter is presented in Chapter 4, and the results obtained from the methodology are presented in Chapter 5.

4

System Design

This chapter presents the hardware design requirements, components and process required to implement Realtek RTL2832U chipset based devices as Passive Bistatic RADAR (PBR) receivers in order to achieve the objectives of the project specification.

4.1 Introduction

This chapter details the system design that was used to develop a passive bistatic RADAR system based upon RTL-SDR dongles as described in Chapter 3. This chapter proposes an overall system model, identifying the key aspects required to develop a suitable hardware configuration, and test the resulting hardware to confirm it functions within the expected parameters. Hardware and software aspects of the hardware configuration, and testing equipment are examined.

4.2 System Model

A system model that encompasses the design requirements of an RTL-SDR based passive bistatic RADAR has been addressed. The model contains five (5) design elements that were addressed in the design process. The design elements are addressed in Sections 4.4 to 4.16. These design elements cover hardware requirements, software requirements, and external validation requirements that are necessary to confirm the operation of the passive bistatic RADAR. The system model is presented in Figure 4.1.

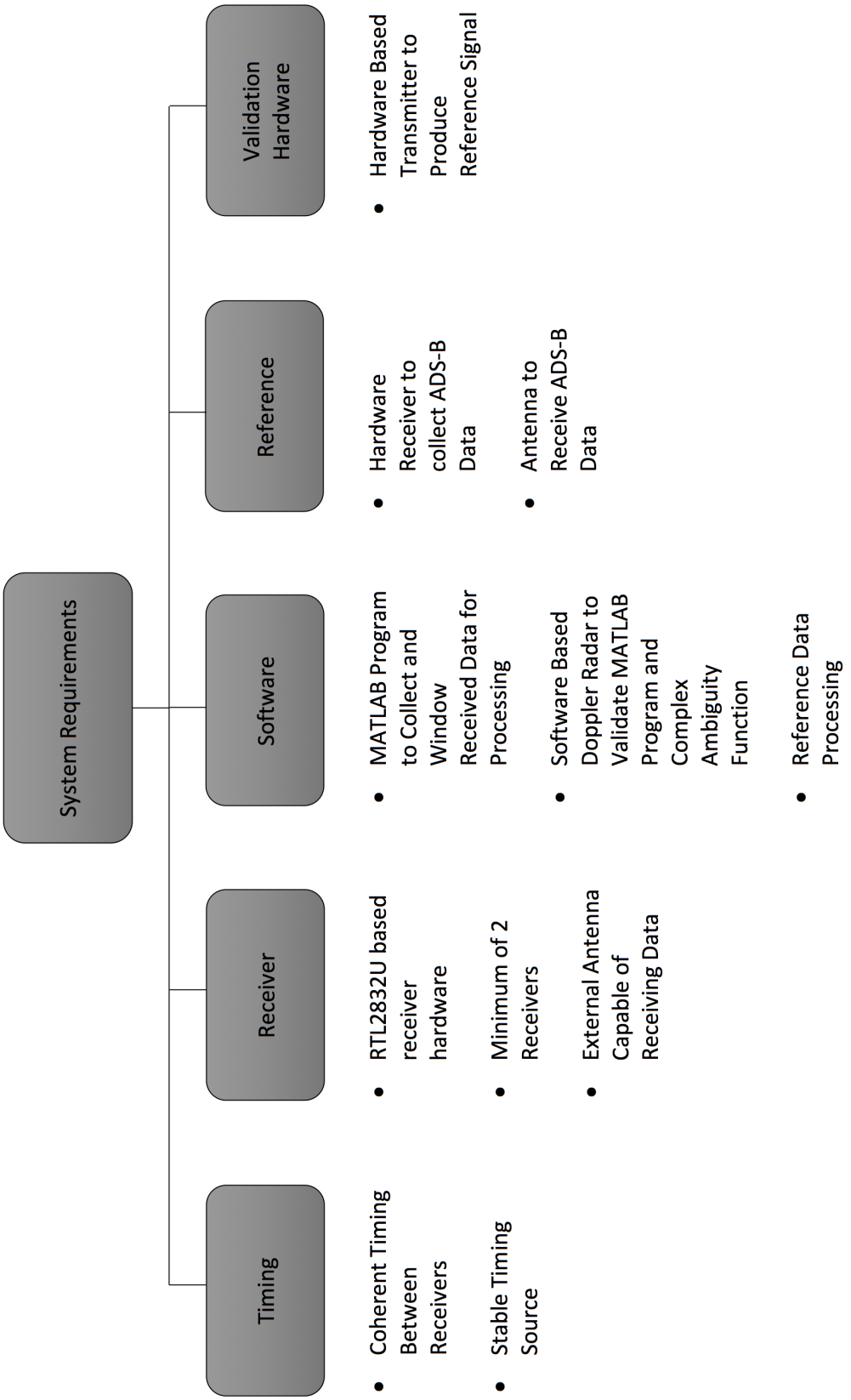


Figure 4.1: Low Cost Passive Bistatic RADAR System Requirements.

4.3 System Design Flow Chart

A system design flow chart that encompasses the design process undertaken to design an RTL-SDR based passive bistatic RADAR has been developed. The flow chart outlines the process threads required to develop a functional PBR. Each stage of the design process has been addressed in Sections 4.4 to 4.16. The system design flow chart is presented in Figure 4.2.

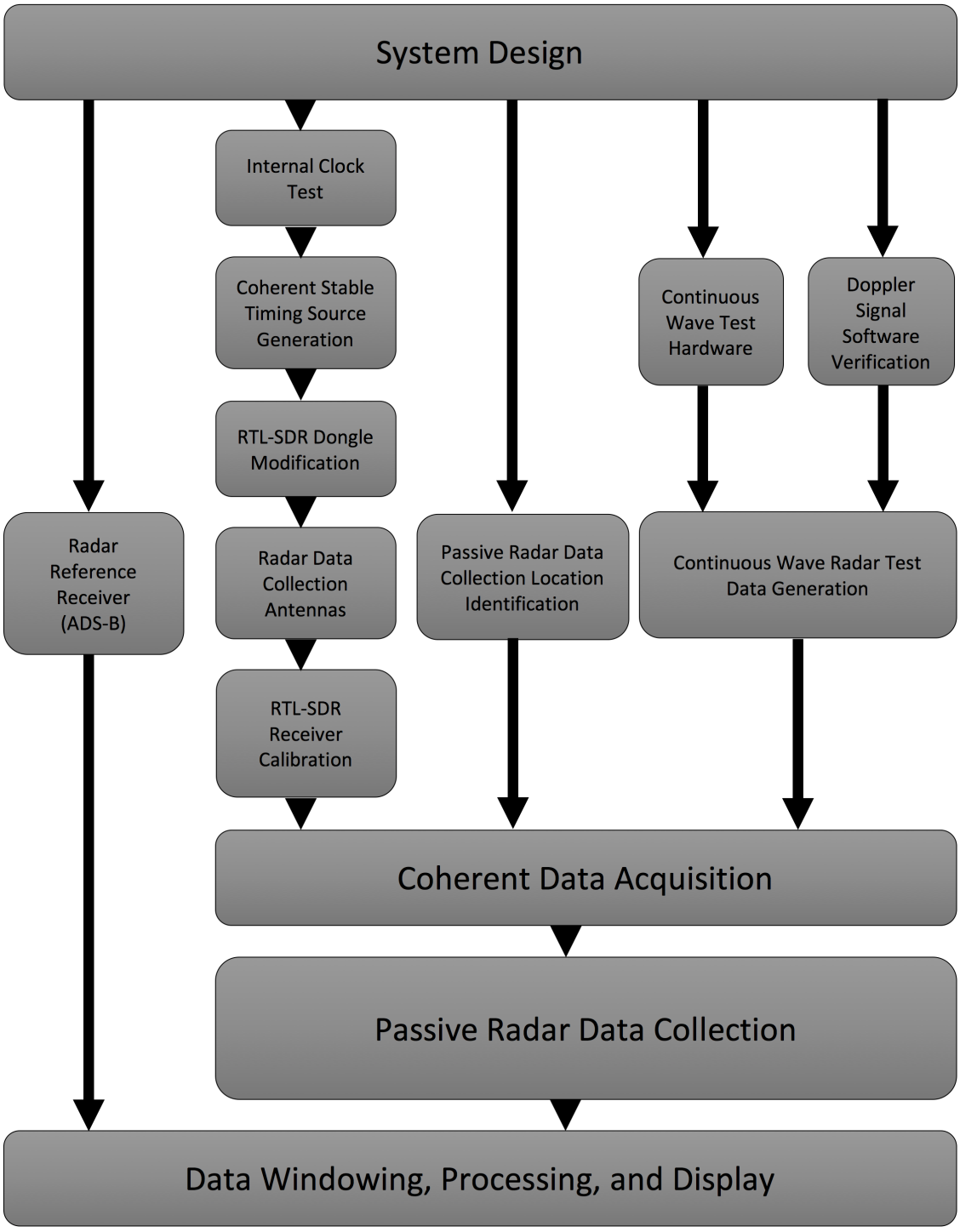


Figure 4.2: Low Cost Passive Bistatic RADAR System Design Flow Chart.

4.4 Coherent Stable Timing Signal Generation

Based upon the results of the internal RTL-SDR timing source testing in Section 5.3, an external, stable clock generation source was identified as the minimum requirement to achieve the required hardware design stability. From the identified options listed in Section 2.4.3, the Arduino based Si5351a Voltage Controlled Oscillator was determined to be the most suitable for use, based upon its low cost, and availability.

In order to reduce the overall footprint and power requirements of the design, and ensure that it can be contained to a single 10-port USB hub, the Freetronics Arduino compatible Leostick was identified as a suitable Arduino device to which the VCO could be controlled from. Figure 4.3 shows the Freetronics Arduino compatible Leostick. The device is based on the Genuine Arduino Leonardo, however, was substantially modified to reduce the footprint sufficient that it will fit in the form factor of a USB flash drive, and is capable of connecting directly to a USB port. A full schematic of the Freetronics Leostick is presented in Appendix E.

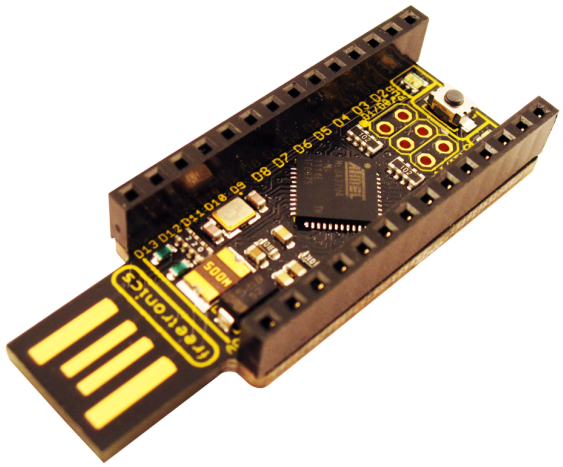


Figure 4.3: Freetronics Arduino Compatible Leostick (Oxer & Alexander 2011).

The Si5351 Voltage Controlled Oscillator was mounted onto a suitably sized Freetronics Prototyping board, identified in Figure 4.4, for easy manipulation and modification where required.

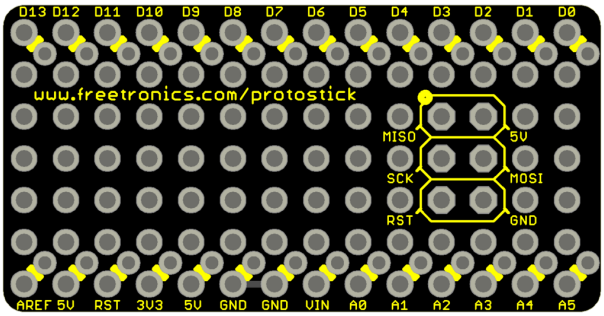


Figure 4.4: Freetronics Leostick Prototyping Board (Oxer & Alexander 2011).

Figure 4.5 shows the completed prototyping board from the top side, and Figure 4.6 shows the board from the underside.

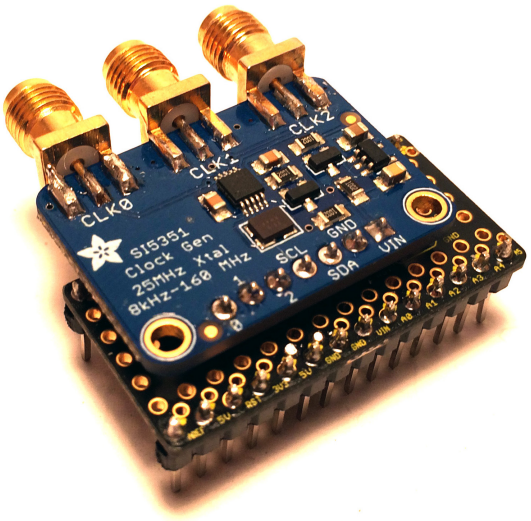


Figure 4.5: Top View of Si5351 VCO Mounted to Freetronics Leostick Prototyping Board.

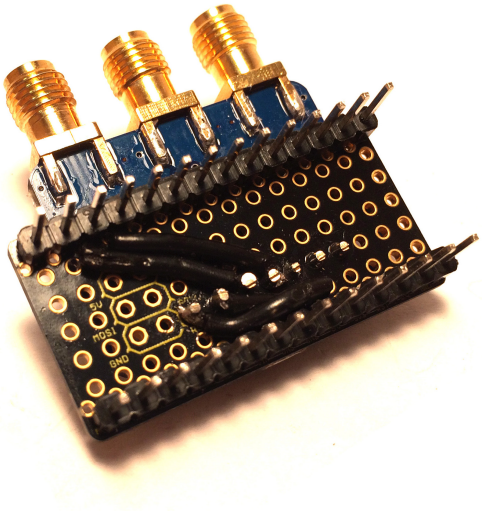


Figure 4.6: Underside View of Si5351 VCO Mounted to Freetronics Leostick Prototyping Board.

It can be noted in Figure 4.6, that of the total 7 interconnections presented on the Si5351 VCO, only 4 are in use. Table 4.1 identifies the interconnections between the Si5351 breakout board, and the Freetronics Leostick.

Si5351 Pin	Leostick Pin
VIN	5V
GND	GND
SDA	D2
SCL	D3

Table 4.1: Si5351 VCO Breakout Board to Freetronics Leostick Interconnections.

Finally, the assembled Freetronics Leostick and Si5351 development board are shown in Figure 4.7.

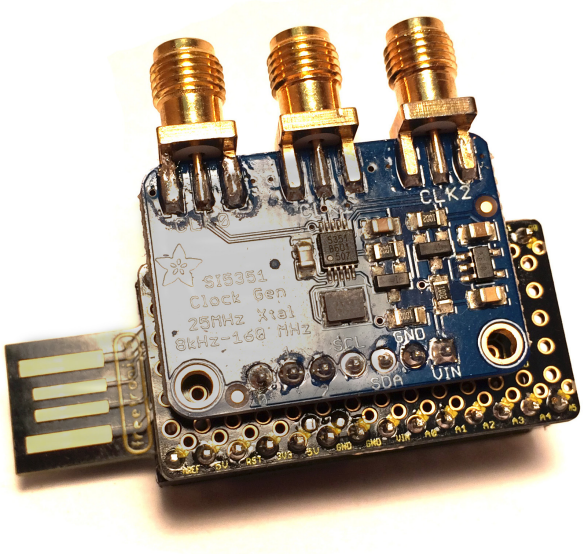


Figure 4.7: Assembled External Timing Source Generator.

Generating a timing signal at the requisite 28.8 MHz requires an Arduino Sketch developed in the Arduino programming environment. The program is based upon the Adafruit Si5351 library, and makes use of fractional multiples of the VCOs onboard 25MHz clock. The Si5351 employs the use of a Phase Locked Loop (PLL) to maintain clock stability, unlike the onboard clock source of the RTL-SDR dongles. The PLL is set by the formula:

$$PLL\ Frequency = 25\ MHz \times Integer\ Multiplier + Fraction\ of\ Multiplier \quad (4.1)$$

$$PLL\ Frequency = 25\ MHz \times 32 + \frac{32}{125} \quad (4.2)$$

$$PLL\ Frequency = 806.4\ MHz \quad (4.3)$$

Subsequently, each output frequency is defined by:

$$Output = \frac{PLL}{Divisor + Fraction\ of\ Divisor} \tag{4.4}$$

$$Output = \frac{PLL}{28 + \frac{0}{1}} \tag{4.5}$$

$$Output = 28.8MHz \tag{4.6}$$

It was important to note that the Si5351 breakout board contains 2 PLLs and in order to attain coherence between receiver dongles, they must all receive their clocking signal from the same PLL. The code contained in Appendix F was used to generate the timing signals used in the collection of data throughout this project.

4.5 RTL-SDR USB Dongle Modification

The standard RTL-SDR dongle identified in 2.4.2.4 was the subject radio receiver for this research. As shown in Figure 4.8, it is not suitable as a Passive Bistatic RADAR (PBR) receiver in its original form due to the obscure antenna input, and the lack of a coherent external timing input.

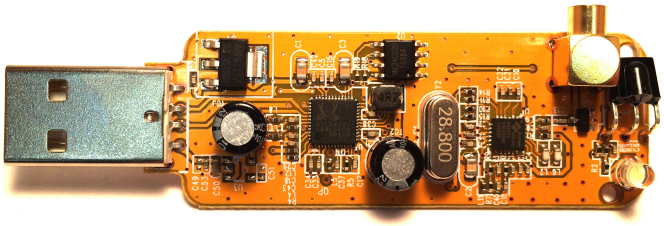


Figure 4.8: Unmodified RTL-SDR USB TV Tuner Dongle.

As it was necessary to receive both a reference signal, and a surveillance signal, two receivers were required, and hence the requirement for a coherent timing source as described in Section 2.4.3. In order to interface the external timing source to the receivers, and to allow greater interoperability of the receiver, a number of modifications need to be made. These modifications were:

- replacement of the existing MMCX antenna connector with an SMA connector;
- removal of the 28.8 MHz crystal oscillator;
- modification of the circuit board to accommodate the installation of an additional SMA connector;
- installation of an Edge-Launch SMA connector for interfacing to the external timing signal generator; and
- installation of an R-C filter circuit to interface the external timing signal generator to the existing crystal oscillator connection point.

In undertaking the rework of the RTL-SDR dongles, it was important to maintain a proper technique, ensuring that where desoldering was occurring, solder wick was used to absorb the excess, and no individual component was overheated. Overheating can reduce the operational ability of a component, inducing either a reduced functionality or a complete failure, hence, there was a need for strict oversight during the re-work process. Additionally, due to the large amount of smoke generated whilst removing components from reheating solder, and the unknown origin of the solder manufacture, primarily, whether lead-free solder had been used in the original construction, appropriate safety measures, including the use of a filtered extraction fan and safety glasses, were employed to maintain safety during the rework process.

Figure 4.9 shows the RTL-SDR board with all of the necessary components removed, and the board cleaned, readied for installation of new components.

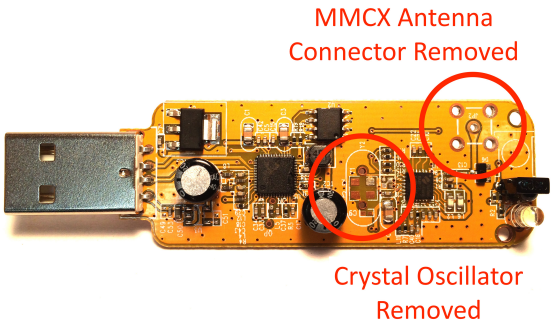


Figure 4.9: RTL-SDR USB TV Tuner Dongle Stripped of Excess Componentry.

Figure 4.10 shows the circuit board modified to strip back a sufficient area of solder mask that an SMA edge-launch connecter can be attached, allowing interface to the external timing source.

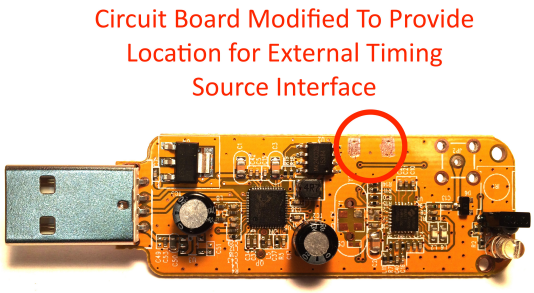


Figure 4.10: RTL-SDR USB TV Tuner Dongle Showing PCB Modification for Edge-Launch SMA Connector.

Finally, Figure 4.11 shows the RTL-SDR dongle with modifications complete, including:

- an SMA connector fitted in-lieu of the original MMCX connector at the antenna fitting, allowing interface to a wider range of antennas and adapters;
- the installation of an edge-launch SMA connector for connection to the previously described external timing source; and
- installation of an R-C filter comprising of a 28Ω resistor between the clock signal input and the ground plane, and a 10 nF capacitor linking the external clock input to the original crystal input location on the circuit board.

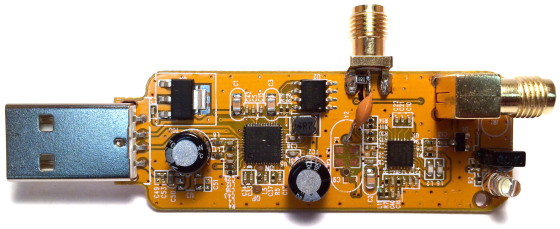


Figure 4.11: RTL-SDR USB TV Tuner Dongle Showing All Necessary Modification Completed.

A total of three (3) dongles were modified for the project, providing the two necessary for acquisition of both reference signals and surveillance signals for RADAR and a third dongle as a redundancy, should either of the other two fail, either in testing or in use. The modified dongles were tested in accordance with the methodology described in Section 3.4.3 with the results in Section 5.5.

4.6 Completed Hardware Device

The completed Hardware configuration consists of two modified RTL-SDR dongles attached to a 10 port USB hub. The external timing signal generation circuit is also attached to the hub, and connects to the RTL-SDR dongles via 150mm SMA plug to plug patch leads. The 10 port USB hub is externally powered from a 5 volt 2 amp power supply, which is sufficient to support additional dongles. The configured hardware attaches to any computer via a single USB cable. This configuration limits the potential for any coherence loss from the two receivers, reducing the software cross-correlations

burden. The two dongles have been fitted with SMA to BNC adapters, in order to facilitate connection to external antennas. The configured hardware device is shown in Figure 4.12.

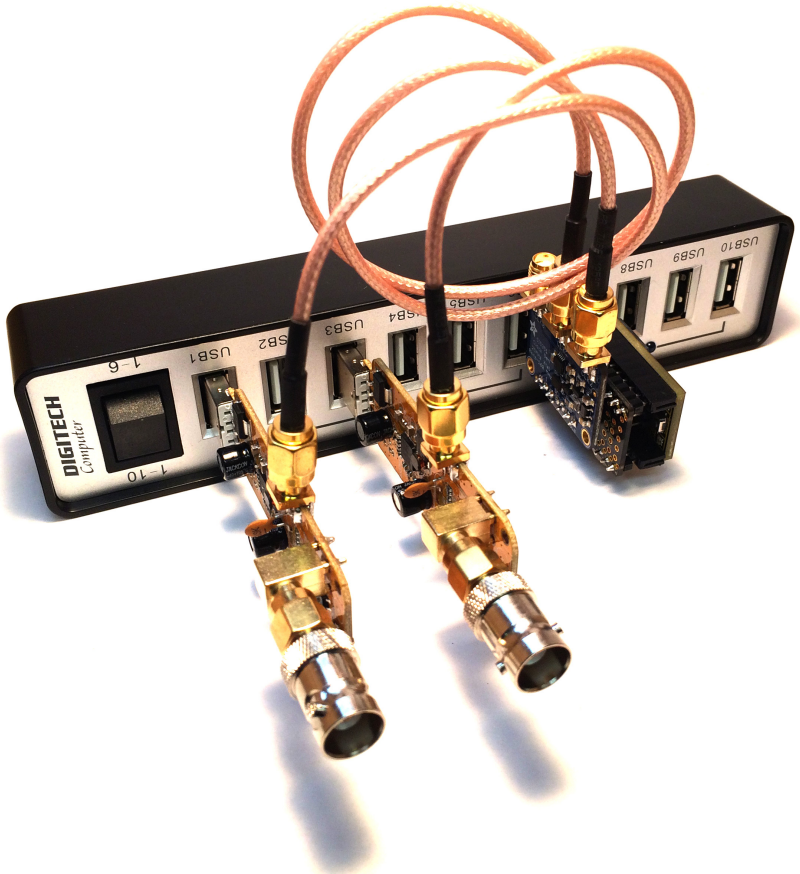


Figure 4.12: RTL-SDR USB TV Tuner Dongle Showing All Necessary Modification Completed.

4.7 RADAR Data Collection Antennas

Each RTL-SDR dongle is supplied with a small antenna, suitable for use in countries with high density accomodation, and a large number of television broadcast transmitter

sites, covering substantially smaller areas than those covered in Australia. The antenna is approximately 105mm long, and, assuming that the antenna is a quarter wavelength dipole, is designed to have a centre frequency of:

$$f_c = \frac{C}{\lambda} \tag{4.7}$$

$$f_c = \frac{3 \times 10^8}{0.105 \times 4} \tag{4.8}$$

$$f_c = 714.29MHz \tag{4.9}$$

Given that Digital Video Broadcast - Terrestrial (DVB-T) signals in Australia cover a range spanning from the bottom of Band I at 47MHz to the top of Band V at 806MHz. The frequencies of interest in Sydney, New South Wales, where testing was undertaken, primarily span a range within 177MHz to 227MHz, the gain of the antenna over the region of interest was not sufficient to provide reasonable results. The antenna provided with the RTL-SDR dongles is shown in Figure 4.13 for reference.

Figure 4.13: Quarter Wave Dipole Antenna Supplied with RTL-SDR Dongle.

In order to ensure a suitable dataset could be achieved over the required range, two 32 element log periodic antennas were sourced to undertake testing. The antennas have an impedance of 75Ω to match the input impedance of the RTL-SDR receivers, and are designed to cover the requisite Australian television bands. The antennas are capable of receiving signals within the range identified in Table 4.2.

Band	Channel	Gain	Frequency Range
VHF	5-12	8dB	174MHz to 232MHz
UHF	21-69	8.5dB	470MHz to 862MHz

Table 4.2: Passive Bistatic RADAR Receive Antenna Characteristics.

The receive antennas were mounted on portable tripods in order to maintain portability and flexibility to attain a suitable signal. The antennas were interfaced with the RTL-SDR receiver from the internal antenna balun via RG6 quad-shield coaxial cable. This ensures there is minimal loss between the antenna, and the receiver. One of the configured receive antenna is shown in Figure 4.14

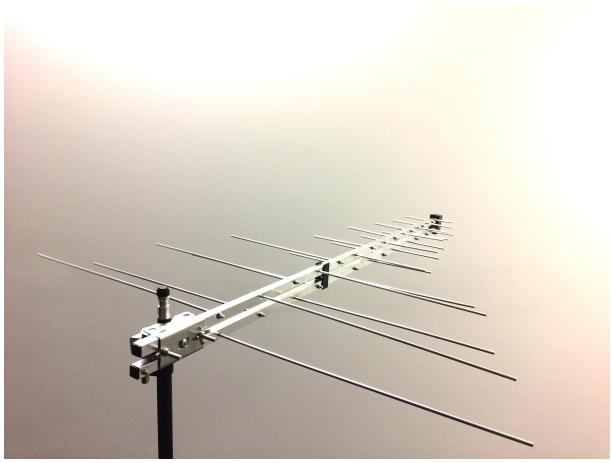


Figure 4.14: Configured 32 Element Log Periodic Receive Antenna.

4.8 RADAR Reference Receiver

To ensure that any received RADAR signal is actually the intended target, and not spurious noise or interference, it was necessary to have a reference data set, as described in Section 3.2.3. For the purpose of this project, commercial aircraft were identified as the most abundant and easily identifiable RADAR receiver targets. To correlate their locations with what is being calculated by the RADAR receiver, two software applications, and a purpose built antenna were implemented to verify the received surveillance signal data.

Data was collected from the ADS-B beacons of commercial aircraft within the expected RADAR receiver range through two existing freeware programs. RTL-1090, and Virtual Radar Server. RTL-1090 was developed by (Jetvision.de 2014) as a non tunable 1090 MHz receiver application for Mode-A/C and Mode-S ADS-B data. Its design is intended to ensure it has a low use of resources, and it is capable of running multiple instances. The applications primary intended purpose is to receive aircraft beacon data for interfacing with additional software that is capable of interpreting and overlaying the received data on a map. As such, RTL-1090 outputs all the data that is received over both TCP and UDP ports. A screenshot of the RTL-1090 interface is presented in Figure 4.15.

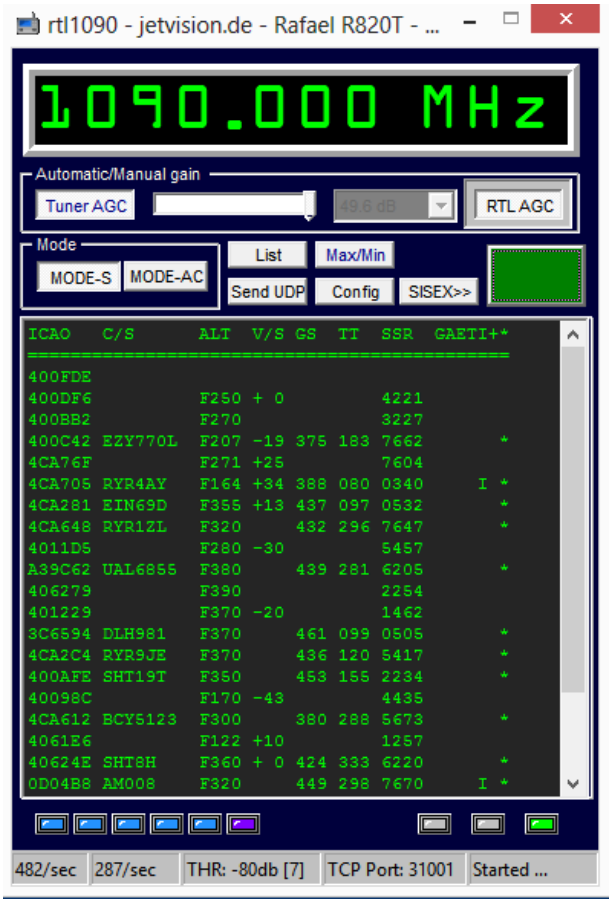


Figure 4.15: RADAR Reference Data RTL1090 Data Acquisition Receiver.

Virtual Radar Server provides the requisite interface to the data received by RTL-1090. It was developed by Whewell (2010), with the intent of overlaying the data received from the aircraft on a Google Map, for clear interpretation. The collated data is packaged into a web server, which can be accessed locally on a defined port, or, dependent upon routing settings, the data may be made available to the wider internet. For the purposes of this project, the collected data was used locally to match aircraft position to any doppler or range shift identified within the decoding algorithm. A screenshot of the Virtual Radar Server application has been omitted as it consists primarily of configuration options, and does not provide any relevance. A screenshot of the collated data from both RTL-1090 and Virtual Radar Server as viewed from Google Chrome is shown in Figure 4.16.

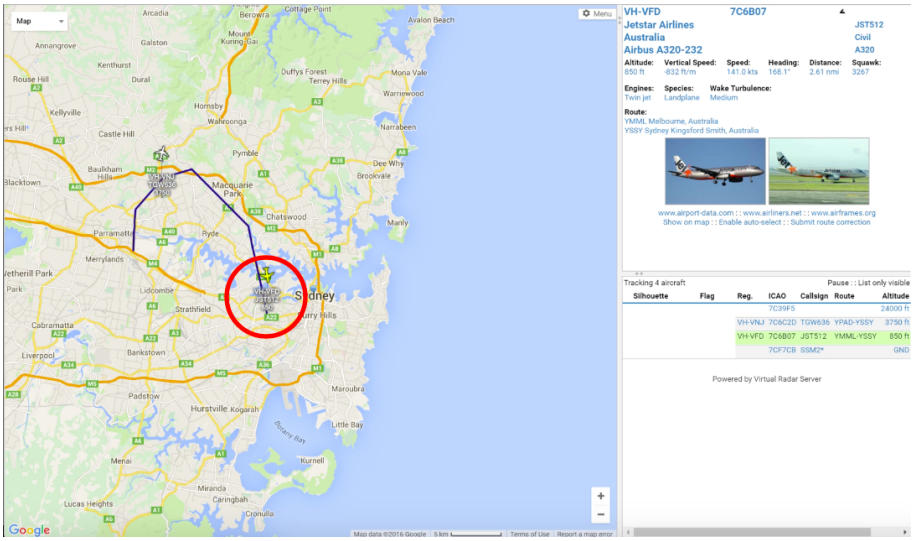


Figure 4.16: RADAR Reference Data from Virtual Radar Server in Google Chrome.

The transmission frequency of ADS-B data from aircraft is 1090 MHz, in order to acquire as much data as possible over the estimated receive area, a dedicated antenna was manufactured. The antenna design was based on a quarter wave spider beam antenna, as shown in Figure 4.17. The length of each element corresponds to a quarter wavelength of 1090 MHz as defined by:

$$\lambda = \frac{C}{f_c} \tag{4.10}$$

$$\lambda = \frac{3 \times 10^8}{1090 \times 10^6} \tag{4.11}$$

$$\lambda = 0.275\ M \tag{4.12}$$

$$\frac{\lambda}{4} = 68.8\ mm \tag{4.13}$$

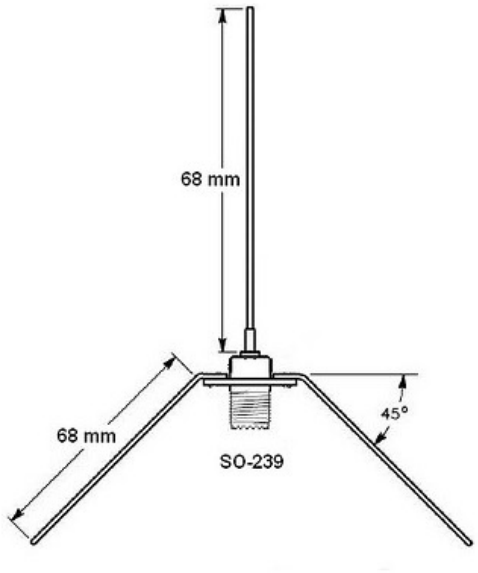


Figure 4.17: 1090 MHz Spider Beam Antenna Arrangement.

Assembly of the spider beam antenna consists of an SO-239 socket, primarily used on RF devices as an antenna connector, placed so as the connection interface points downwards, with the main element soldered to the centre pin of the connecter. Ground plane elements are soldered onto the outside of the connector at intervals of 45°, then bent downwards at 45°. The completed antenna, utilised for the project is shown in Figure 4.18. Note that the hook shown on the completed antenna was for mounting purposes only, however it will have a minor and negligible effect on the antenna performance at 1090 MHz.

Figure 4.18: Configured RADAR Reference Receiver Antenna.

4.9 Continuous Wave Testing Hardware

To verify the general operation of the developed Passive Bistatic RADAR (PBR) receiver, testing was conducted in a controlled environment. It was determined that the testing required only needed to be sufficient to verify the operation of the receiver, and determine the operation of the implemented software decoding algorithm. This determination was based on the low cost objective of the project. Had a full functionality test been required, a device such as the Blade-RF or USRP identified in Section 2.4.2 would need to be configured as a transmitter that was producing the requisite FM or OFDM to match the input requirement under test.

The continuous wave target identification abilities of the PBR receiver was investigated through the development of an Arduino based 433 MHz continuous wave transmitter. Employing the functionality of a 433 MHz Amplitude Shift Keying (ASK) transmitter module interfaced to an Arduino Uno, a continuous wave output was produced. Although no range data would be discernible from the device whilst under test, the result was

intended to be sufficient to identify doppler shift and therefore, verify that the hardware and software implementation were capable of their intended purpose as a Passive Bistatic RADAR (PBR).

As the most prevalent Arduino device, upon which the majority of devices are tested and developed, an Arduino Uno was chosen as the micro-controller platform from which the transmitter module would operate. The Arduino Uno is readily available, and capable of producing the requisite outputs to interface to the transmitter module. A full schematic of the Arduino Uno is presented in Appendix G.

The 433 MHz transmitter module used to conduct testing is commonly used in an On-Off Keying (OOK) configuration, and whilst labelled as ASK, it is technically not capable of that output. The modulation frequency and amplitude are fixed, and the device is switched in and out based on simple data transmission structures that are sent to it via the attached micro-controller. The transmission method employed by the device is commonly used in RF remote controls and basic telemetry devices.

In a similar method to that used to construct the external timing circuit, the 433 MHz transmitter was mounted onto an Arduino Uno compatible Freetronics Prototyping board, identified in Figure 4.19, allowing an easy and interchangeable interface to the Arduino Uno device.

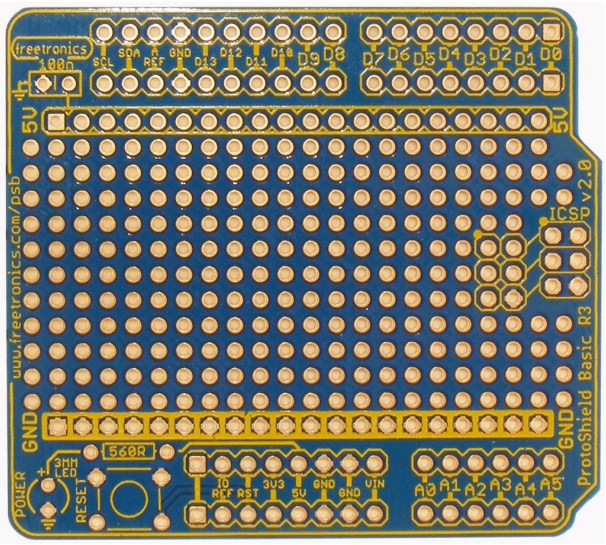


Figure 4.19: Freetronics Uno Prototyping Board (Oxer & Alexander 2011).

Figure 4.20 shows the completed prototyping board from the top side, and Figure 4.21 shows the board from the underside.

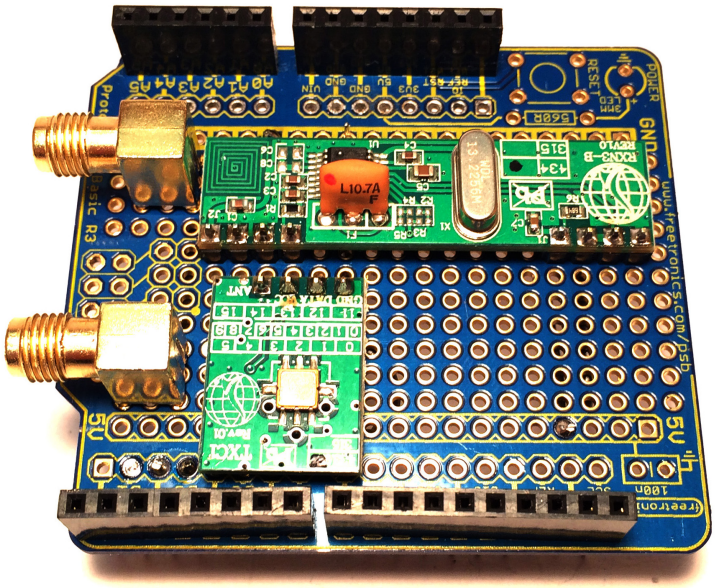


Figure 4.20: Top View of 433MHz Transmitter Mounted to Freetronics Uno Prototyping Board.

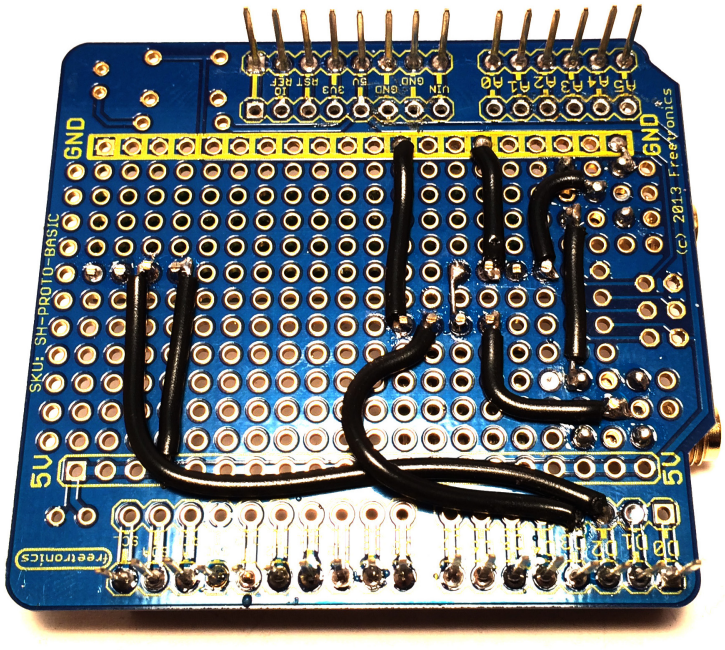


Figure 4.21: Underside View of 433MHz Transmitter Mounted to Freetronics Uno Prototyping Board.

Figure 4.22 shows the 433 MHz transmitter interface mounted to the prototyping board. It can be noted that there are 4 interconnections on the 433 MHz transmitter board.

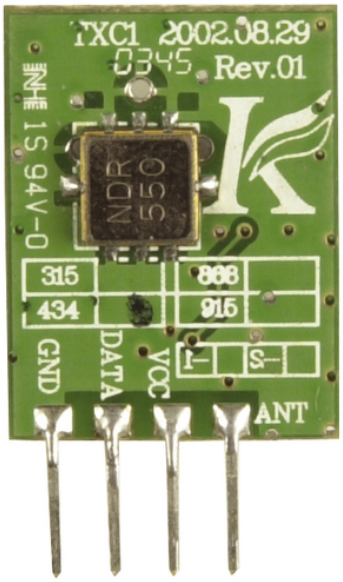


Figure 4.22: 433 MHz OOK RF Transmitter Circuit for Arduino Interfaces.

Table 4.3 identifies the interconnections between the 433 MHz transmitter board and the Arduino Uno.

433 MHz TX Pin	Arduino Uno Pin
GND	GND
DATA	D3
VCC	5V
ANT	External Antenna

Table 4.3: 433 MHz Transmitter Board to Arduino Uno Interconnections.

Finally, the assembled Arduino Uno and 433 MHz transmitter are shown in Figure 4.23. The configured hardware in the image depicts both a transmitter and receiver that were placed on the prototyping board, however, for this project, only the transmitter functionality has been implemented. The Transmitter has been connected to an external 3.5dBi antenna, in order to increase the reliability and overall power of the transmitter circuit.

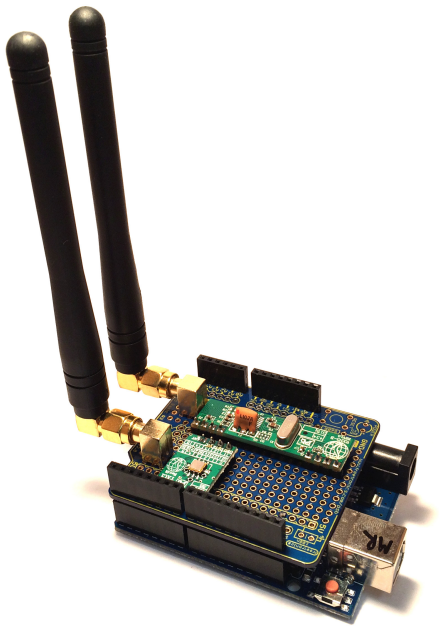


Figure 4.23: Configured Arduino Uno Continuous Wave Testing Hardware Device.

Generating a continuous ASK modulated RF output requires an Arduino sketch developed in the Arduino programming environment. The program is very basic, and is manually manipulated to control the output of the data pin as being either high or low, with high generating an output, and low stopping the output. It must also be noted that the transmitter is designed for short output bursts and not continued operation, thus, the heat of the circuit must be monitored whilst it is transmitting continuously. The code contained in Appendix H was used to generate a continuous output wave for testing.

4.10 RTL-SDR Receiver Calibration

To determine the coherence of the hardware RADAR receivers, and subsequently identify the total frequency offset that occurs as a result of the external timing source, it was necessary to calibrate the two RTL-SDR dongles. This calibration was achieved using an application designed by (Lackey 2010) and modified for RTL-SDR hardware by (Markgraf 2012). The program, called Kalibrate-RTL (Markgraf 2012), exploits GSM frequency correction techniques as described in Section 3.4.4 to determine the frequency offset of the timing source in parts per million (PPM).

The program conducts a scan of the GSM band to determine the available frequencies, then, making use of the GSM Frequency Correction channel, determines the offset of the timing source. This process was carried out for each dongle in turn, with the results from a shared clock source expected to be the same.

Generally, an offset from the desired clock frequency is expected, as the hardware being used is not of sufficient quality to negate all errors. As long as the error obtained is consistent across all dongles tested, the external clock source can be considered to be calibrated and coherent. Results from the dongle calibration identified a consistent offset of -14.9 ppm on any dongle calibrated, thus, the external timing source variation from 28.8 MHz is -14.9 ppm.

4.11 Doppler Signal Software Verification

Verification of any software RADAR decoder is essential in determining the functionality and suitability of the developed program. In order to test the functionality of any

passive RADAR software implementation, a simple doppler RADAR configuration was used. The basic configuration was developed in GNU Radio, and uses a signal produced through computer speakers as the device transmitter. The computer microphone is then used to receive the sound, from which the return will be affected by any object moving toward or away from it. The resulting data files, one for each transmit and receive, are stored for interpretation by other software implementations.

The GNU Radio Flowgraph consists of a sine wave and cosine wave generator, producing the requisite quadrature and in-phase complex output at the computer speakers, and additionally linked to a file sink to store the reference signal. A microphone source block is then used, and connected similarly to a file sink to produce the surveillance signal. Essentially, the program produces a sound at the upper limits of the functional range of the computer speakers, then uses the in-built microphone to receive reflections of that signal, in much the same manner that a conventional RADAR operates, except using an audible frequency. The intention of the implemented program was to receive a valid doppler shift, and process the data through the developed MATLAB program to ensure correct operation. A copy of the basic Flowgraph used to generate doppler RADAR data is presented in Appendix I, and the results of the Doppler signal software validation are presented in Section 5.8.

4.12 Coherent RTL-SDR Data Acquisition

Whilst a shared stable clock source was necessary to achieve signal coherence with RTL-SDR receivers, it has been established previously within this dissertation that there will still be an error induced due to the way in which the processing computer's universal serial bus interfaces with each receiver. This error can be mitigated a number of ways, either through the use of the cross correlation function in MATLAB, or, more accurately at the time of acquisition through the Multi-RTL Out of tree GNU Radio Module. In

this context, an out of tree GNU Radio Module is one which does not live within the GNU Radio source file, that is, a module that has been developed externally to the GNU Radio project.

The module was developed by Krysik (2016) with the original intent of capturing GSM uplink and downlink channels concurrently, as the two frequencies fall outside the bandwidth of a single RTL-SDR receiver. The method implemented by Krysik (2016) in the Multi-RTL block follows the process:

- tuning both RTL-SDR dongles to the same frequency where a known transmitter exists;
- recording a small number of samples with both dongles;
- calculating the cross-correlation of each dongle with respect to the first identified dongle;
- identifying the position of maximums of cross-correlations in order to estimate the relative delay of the channel;
- correcting the delay to time synchronise the channels with channel 0;
- changing the centre frequency of both dongles to their respective target listening frequency; and
- modifying ancillary parameters associated with each dongle, such as gain.

The resulting output from the module is accurate to approximately ± 1 sample over 500,000 samples. Krysik (2016) showed within the same work that once correlation had been achieved, the centre frequency of a dongle can be changed whilst maintaining that correlation, hence validating the methodology used to implement the Multi-RTL module. Figure 4.24 shows the method used by the Multi-RTL module to correlate data.

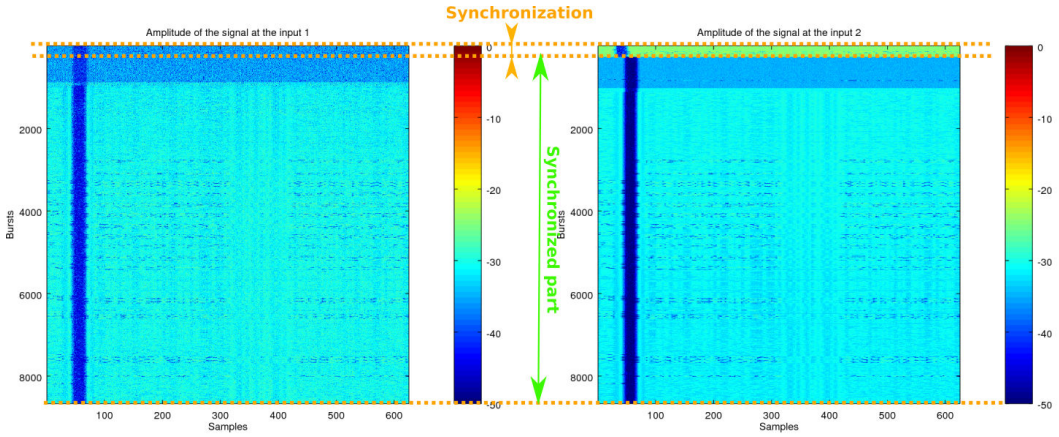


Figure 4.24: Multi-RTL Out of Tree Module Receiver Correlation Process (Krysik 2016).

Data acquired with the Multi-RTL module was stored using a GNU Radio flowgraph developed by Krysik (2016) and distributed with the module. The code is presented in Appendix J.

4.13 Continuous Wave RADAR Test Data Generation

Generation of test data for a continuous wave Doppler RADAR required the implementation of both the continuous wave testing hardware developed in Section 4.9 and the Passive RADAR hardware receiver detailed in Section 4.6. The two devices were configured with a separation of approximately 5 metres, and data was recorded using the method detailed in Section 4.12. The recorded data is presented in Section 5.9.

4.14 Passive RADAR Data Collection: Location Identification

The maximum range of the RADAR receivers is limited by Equation 2.15, which includes reference to the noise floor of the receivers. The overall effectiveness of the hardware configuration under test is also heavily limited by the transmitter power and antenna radiation pattern of the non-cooperative transmitter being used to illuminate potential targets. As aircraft were chosen to be the target of interest, another influencing factor was proximity to an airport and an active flight path. As a result, there were limitations on the possible locations for data collection.

With Digital Video Broadcast - Terrestrial (DVB-T) signals being the main signal of interest, it was critical to the outcome to ensure the location chosen had a high signal strength. The geography of Author's suburb of residence required TV antennas to be mounted on minimum 4 metre mast to ensure clear reception, nor was it within relative proximity to a flight path. Hence, it was determined that it was not a suitable data collection location.

In the current world political climate, where terrorism fears are prevalent, if testing were to be conducted in a public space, the act of pointing large antennas anywhere near aircraft would arouse unnecessary fear in the general populous, and could result in attention from law enforcement. Hence, it was determined that testing would need to be conducted on private property, with permission from the building owner's representative.

With clear access to transmitters as a requirement, and limited options for building access, one location for data collection was identified. The building chosen was 25 storeys tall with a conference room facing to the north, an ideal aspect pointing directly towards the transmitter of interest. The conference room location on the 25th floor provided an elevation of approximately 80 M and provided access to the flight path of

Sydney Airport runway 34, being the main northern approach.

Efforts were made to source additional locations for data collection, noting that the available location has a number of limitations. Field testing conducted on a number of sites, failed to identify a suitable alternative location. Each alternative location tested provided a combination of poor band scan results, meaning that there was not a sufficient transmitter strength, or limited visibility of an active flight path, hence, no target from which to acquire data.

4.15 Passive RADAR Data Collection

Data collection occurred over two consecutive days in accordance with the methodology outlined in Section 3.4.5. In order to maximise the viability of the collected data, a number of different frequencies and signal types were analysed, whilst maintaining a consistent configuration. Data was collected over the frequencies:

- 104.90 MHz FM Radio
- 202.928 MHz DAB+ Digital Radio
- 177.50 MHz DVB-T Digital Television

Data collection occurred using the previously identified Multi-RTL based GNU Radio Flowchart identified in Appendix J. Samples were collected at either 1 Msps or 2 Msps, with a collection time of 60 seconds. This generated 60 million samples for the lower sample rate, and 120 million samples for the higher sample rate, producing file sizes of approximately 450 MB and 900 MB respectively for each channel.

The collected data was saved into files identifying the frequency and given a unique

dataset identifier in order to be processed through MATLAB. From the acquired and processed data, passive RADAR target information extracted.

4.16 Data Windowing MATLAB Program

The data collected contained target identifying information, but required substantial processing in order to extract the information of interest. A MATLAB program was developed to read the collected data, divide it up into suitably sized windows, and ultimately plot the result, where any potential PBR information could be identified.

The collected data was stored in a GNU Radio proprietary data format with the extension ".cfile." Whilst appearing as being proprietary, the file essentially only stores data as comma separated values, but is modified to store complex datasets. The MATLAB program developed reads the ".cfile" and extracts the data into a matrix for manipulation.

The data is subsequently broken into windows of one quarter of a second with a Hamming window, to preserve the nature of the captured data, from which point it can be further processed. Further processing occurs in the form of a correlation verification, validating the correlation that occurs on capture, and determining the validity of the sample. This is followed by a Fast Fourier Transform (FFT) to identify the relevant frequency components of the window.

The final stage of data processing is to pass the collected reference and surveillance sample through the complex ambiguity function. Section 2.2.4 identified that the operation of the complex ambiguity function is beyond the scope of this project, and as such it has been implemented as a function, based upon the work of Johnson (2001). The function developed by Johnson (2001) computes the ambiguity function of the window, and

subsequently plots the result for digestion. MATLAB Code for the Ambiguity function is presented in Appendix K and Appendix L. The MATLAB code used to interpret the collected data is presented in Appendices M and N.

4.17 Chapter Summary

This chapter has presented the system design that was produced from the passive bistatic RADAR methodology developed in Chapter 3. The system design details the process used to develop each element of hardware and software required to implement an RTL-SDR based passive bistatic RADAR. The system design also details elements of additional hardware and software that were required to conduct controlled testing, and to verify the results collected from the configured passive RADAR receiver.

5

Results and Discussion

This chapter presents the results of the hardware analysis in testing the Software Defined Radio (SDR) devices under controlled conditions to determine their suitability as a Passive Bistatic RADAR (PBR) receiver, the results of a controlled RADAR implementation, and the results of field testing, making use of existing terrestrial transmitter sources.

5.1 Introduction

This chapter details the results that were obtained from the passive bistatic RADAR system designed in Chapter 4 and is divided into sections containing the results from a series of verification tests, and subsequently, from testing of the configured system. The results from the verification testing describe the functionality of the internal RTL-SDR clock, and the one developed for coherence in Chapter 4, a validation test on the USB SDR dongles to confirm functionality is equivalent post modification, and testing to determine the device noise floor. Results are presented from testing conducted on the USB SDR dongle, and the software developed to confirm its suitability as a passive bistatic RADAR receiver. Results from the location identification detail the relative signal strength and inherent limitations that result. The results of data collection and processing for three (3) different non-cooperative carriers are presented, and finally, the results are compiled and discussed to draw conclusions.

5.2 External Test Equipment

Where external testing was undertaken, the equipment used has been certified for accuracy. The primary testing device used throughout this research was a Tektronix TDS-3054C Digital Storage Oscilloscope (DSO) which was calibrated on March 9th 2016. Calibration results data for the device is presented in Appendix O.

5.3 Internal Clock Testing

The crystal oscillator supplied as standard fitment on RTL-SDR receivers, whilst suitable for the original intended purpose of tuning DVB-T television broadcasts and FM radio, is suspected to be inaccurate and subject to variation based on temperature. The inaccuracy of the internal timing circuit was tested to confirm this hypothesis, and validate the requirement for an external accurate timing source. Figure 5.1 depicts the test configuration implemented making use of a X10 oscilloscope probe, note that the DSO is not shown in the image, nor is the computer operating the RTL-SDR dongle.

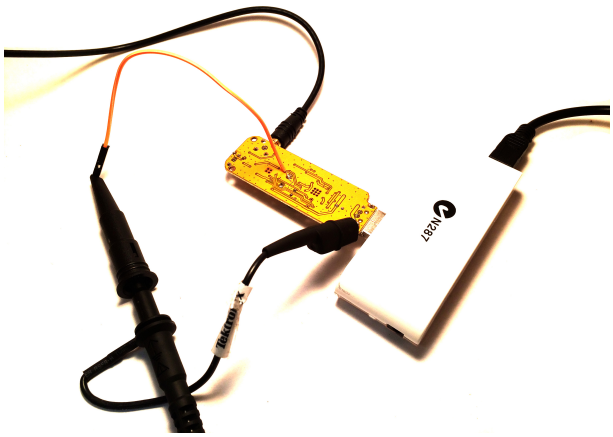


Figure 5.1: RTL-SDR Internal Clock Stability Test Configuration.

The reference frequency requirement for input to the RTL2832U chipset is 28.8 MHz. Testing identified that a variance of 0.1 MHz was sufficient to stop normal device functionality. Figure 5.2 shows the clock frequency variation over one (1) hour from the internal crystal oscillator that forms a standard RTL-SDR dongle. The device was tested at room temperature, however during normal operation, it is expected that the RTL-SDR dongle circuit board temperature will exceed 40°Celsius. No testing was conducted outside the expected ambient temperature of normal operation.

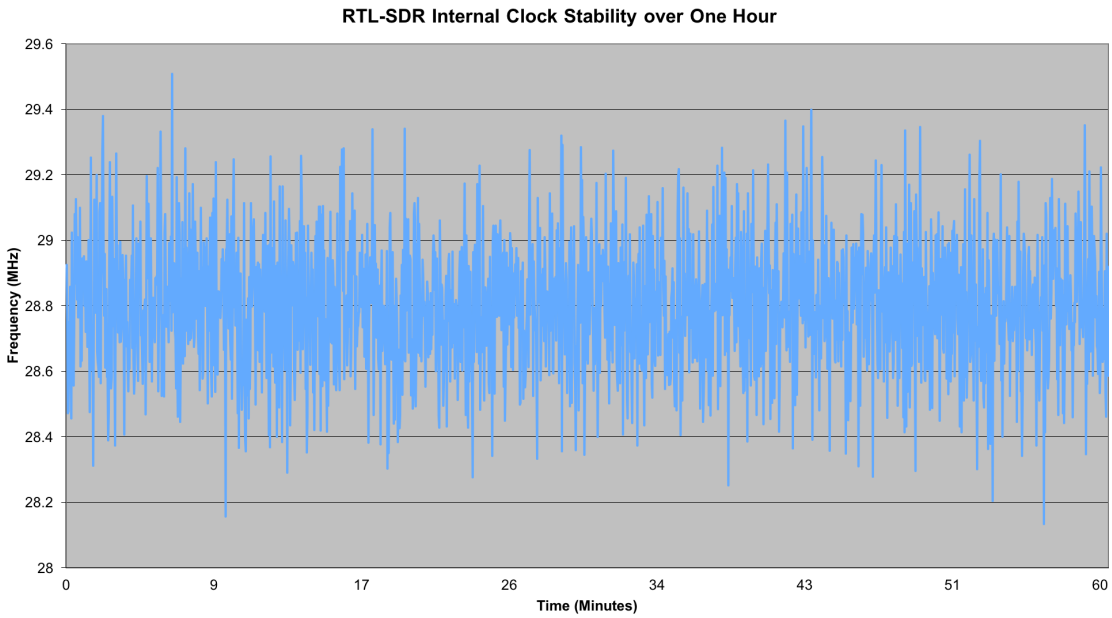


Figure 5.2: RTL-SDR Internal Clock Stability Over One Hour.

Figure 5.3 shows the waveform geometry of the crystal oscillator whilst the internal frequency variation was being monitored.

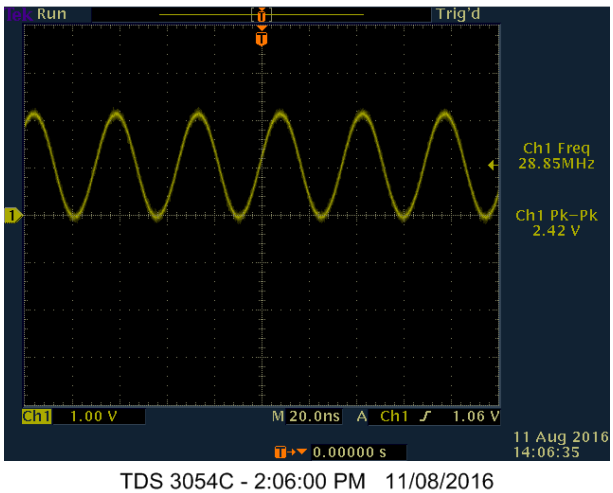


Figure 5.3: RTL-SDR Internal Clock Waveform Geometry.

From the data collected, it can be seen that there is a large instability in the clock source, with a minimum value occurring as low as 28.13 MHz and maximum value occurring at 29.51 MHz. The average value recorded over one hour was 28.8 MHz hence the relatively stable operation of the device. Given the requirement for two devices to share a single timing source, and the relative accuracy required to maintain coherence between the two devices, the results shown confirm that the onboard clock provided with a standard RTL-SDR dongle is **not** suitable for the research requirements. Based on this result, it was determined that an external timing source was required. Section 4.4 describes the hardware design process undertaken to produce a suitable external timing source.

5.4 External Timing Source Testing

The external timing circuit based upon an Si55351 breakout board, as described in Section 4.4 was tested for accuracy following the methodology identified in Section 3.4.1. This is the same methodology as was used for testing the internal timing source. The literature in van de Swaluw (2015) implies that an external timing source will have a greater degree of accuracy, and less prone to unscheduled USB drop-outs. Figure 5.4 shows the clock frequency variation over one hour from the external timing source generator interfaced to a modified RTL-SDR dongle.

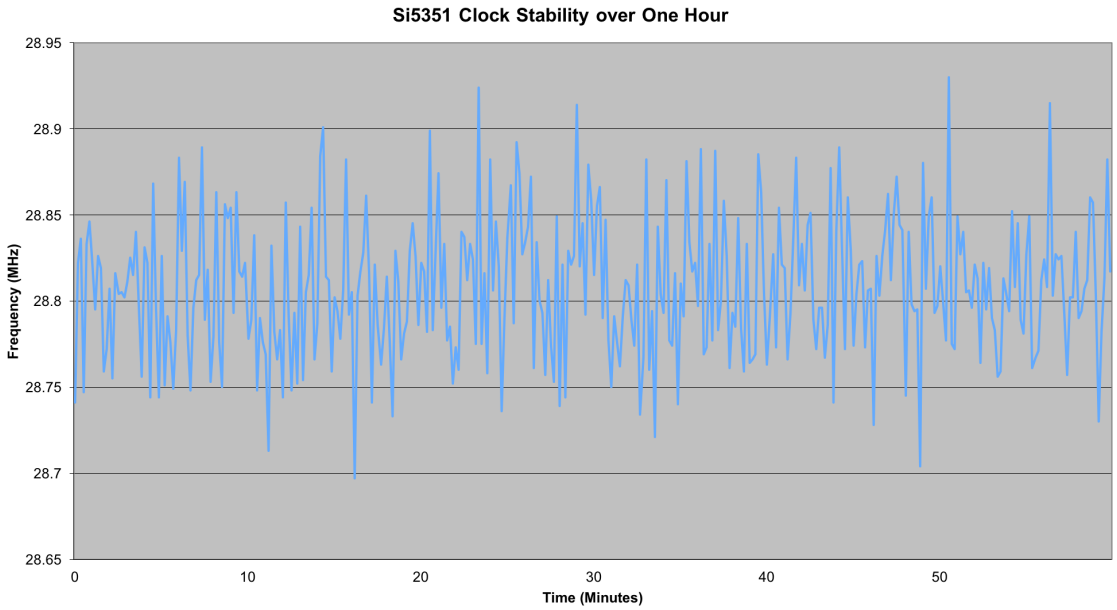


Figure 5.4: Si5351 Breakout Board Clock Stability Over One Hour.

Figure 5.5 shows the waveform geometry of the timing source generator whilst the frequency variation was being monitored.

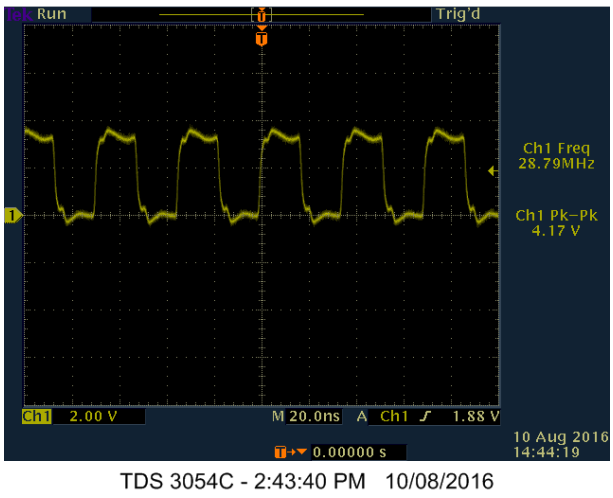


Figure 5.5: Si5351 Breakout Board Clock Waveform Geometry.

The results show substantially less variation over time, with a minimum value occurring at 28.679 MHz and a maximum value occurring at 28.930 MHz. The average value recorded over one hour was, similarly to the internal clock, 28.8 MHz. This represents a range of 0.251 MHz, by comparison, the range of the internal clock source was 1.38 MHz. Therefore, the total variation in frequency over the sampled period (Figure 5.4) is substantially less than that of the internal clock (Figure 5.2), providing a more reliable time source. Whilst it has been identified that when operating multiple dongles coherently, clock deviation within the operating range of the RTL2832U chipset is not significant, so long as it is concurrent to both dongles, the clock stability directly impacts the USB interface, and where it exceeds the tolerance of the RTL2832U chipset, data packets are dropped. Where data is dropped, coherence is lost, hence, a more stable clock provides a better, more accurate result.

It can be noted in Figure 5.5 that the output wave more closely reflects a square wave than the original crystal clock oscillator wave shown in Figure 5.3 due to the circuitry design of the Si5351 VCO. The 820T tuner into which the clock signal is input, is non-discriminate enough to identify this output as a valid clock signal. There is no additional filtering required to reduce the square wave output to match the original crystal oscillator sine wave output.

5.5 RTL-SDR Dongle Validation Testing

To verify that the modifications undertaken on each of the three dongles did not cause any damage to the remaining circuitry, a basic test was undertaken to confirm operation. In accordance with Section 3.4.3, each receiver was tuned to an FM radio frequency to ensure that it was still functioning as it had prior to the hardware changes made in Section 4.4. The FM carrier was arbitrarily chosen as 102.5 MHz because it was within a proximity of approximately 1 km, and therefore, presents the greatest relative

transmitting power at the test location. Figure 5.6 shows the equipment configuration used to conduct validation testing.

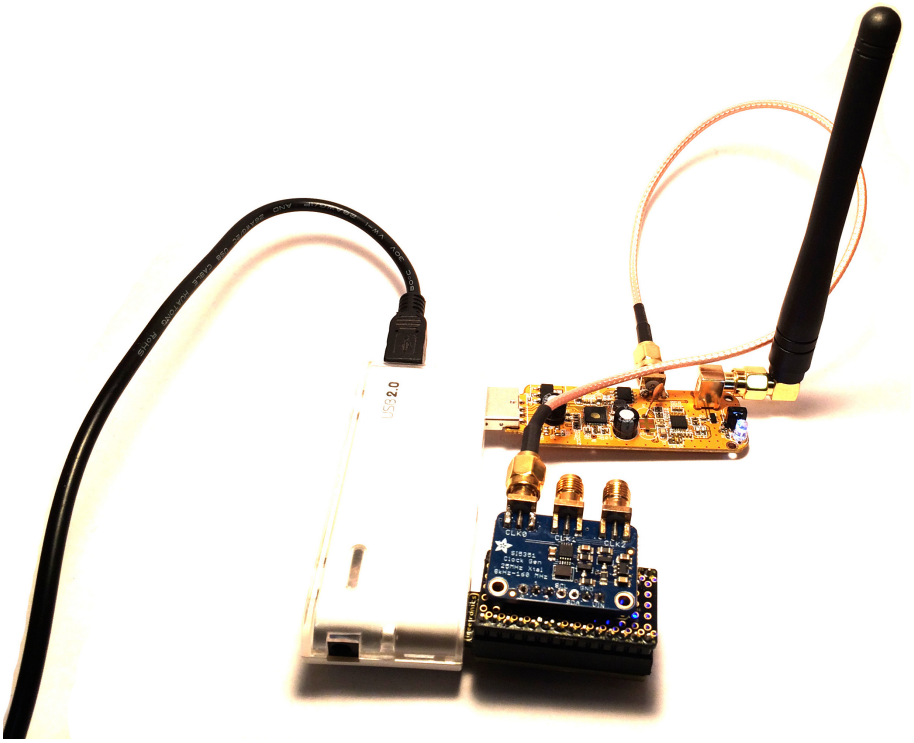


Figure 5.6: Modified RTL-SDR Dongle Validation Testing Configuration.

A screenshot from each test is included for reference. Figure 5.7 shows the validation of dongle 'one,' Figure 5.8 shows the validation of dongle 'two,' and Figure 5.9 shows the validation of dongle 'three.'

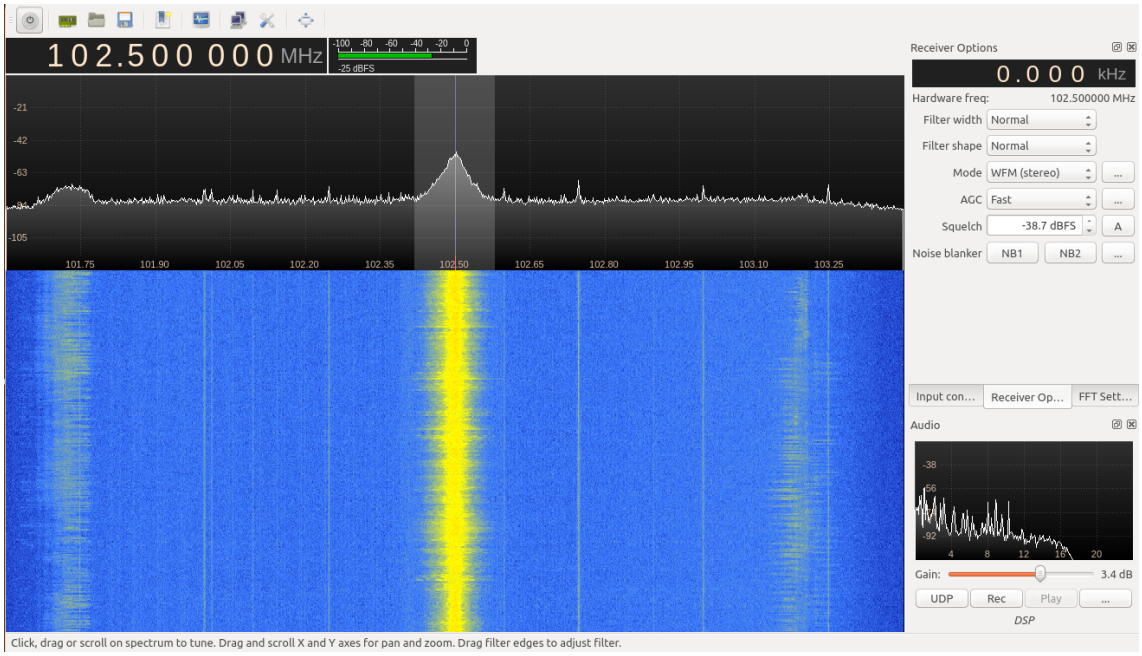


Figure 5.7: Modified RTL-SDR Dongle Number One Validation Test.

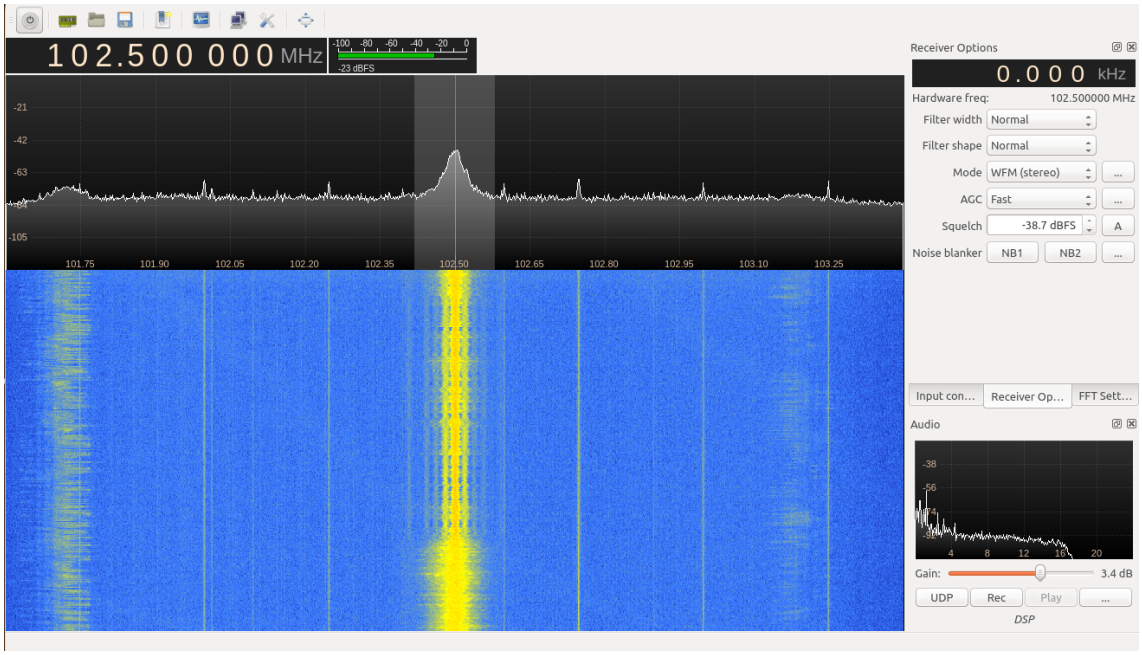


Figure 5.8: Modified RTL-SDR Dongle Number Two Validation Test.

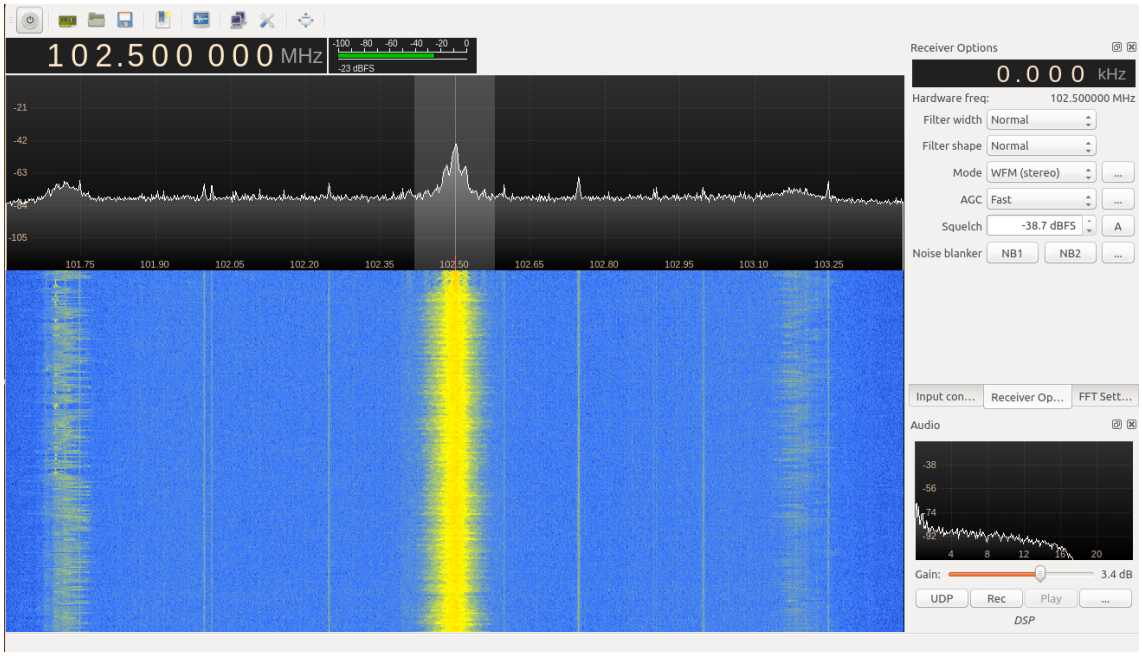


Figure 5.9: Modified RTL-SDR Dongle Number Three Validation Test.

As each of the three figures represents the same result, it can be observed that all three modified dongles are functioning equivalently after modification. Each of the modified dongles are considered suitable for use following modification.

5.6 Radio Receiver Internal Noise Testing

Each modified RTL-SDR dongle was configured with a 75Ω dummy load, and connected to a computer to determine its internal noise floor. Figure 5.10 shows the configuration used to gather noise data. Testing was conducted across the functional range of the RTL-SDR dongle, being 24 MHz to 1.7 GHz, with a gain of 50dB across this range. Data was collected in 1 MHz intervals over a 15 minute period. Noise figure data was generated using the application RTL-power, supplied as part of the modified software

defined radio driver package for RTL2832U based dongles. The terminal command used to initiate data collection was:

```
$ rtl_power -f 24M:1.7G:1M -g 50 -i 15m -1 noise.csv
```

Subsequently, the output data generated in the CSV file was manipulated into a two-dimensional form with the use of a data flattening tool developed by (Keen 2008) called flatten.py.

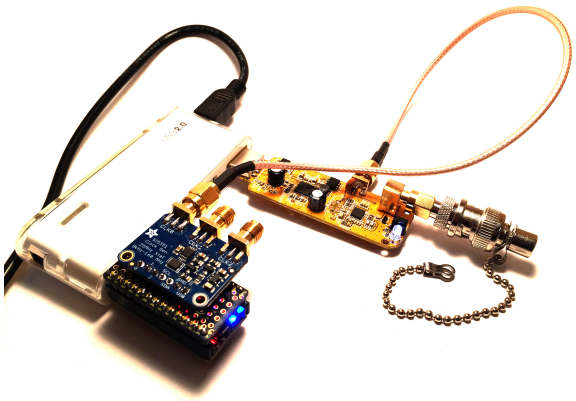


Figure 5.10: Modified RTL-SDR Dongle Internal Noise Figure Testing Configuration.

The results for the noise floor testing are shown in Figures 5.11, 5.12, and 5.13. Note the repeating overtones and large noise bump. The gradual decay over the receive range is also representative of the receiver sensitivity across the band. The Y-axis of each plot represents the power level of the noise in dB relative to the intensity of other noise present, and the prevailing noise floor.

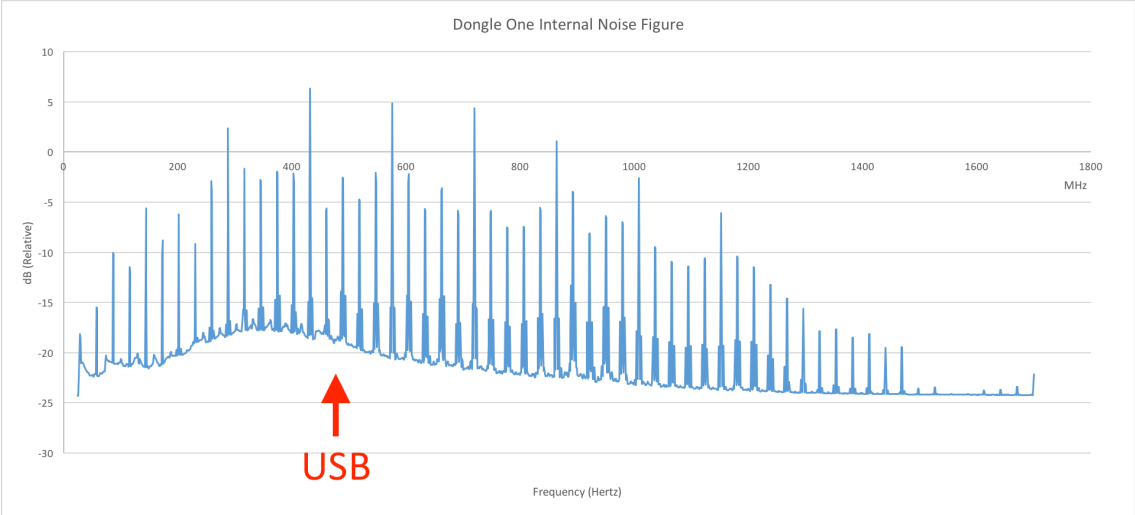


Figure 5.11: Modified RTL-SDR Dongle Internal Noise Figure: Dongle One.

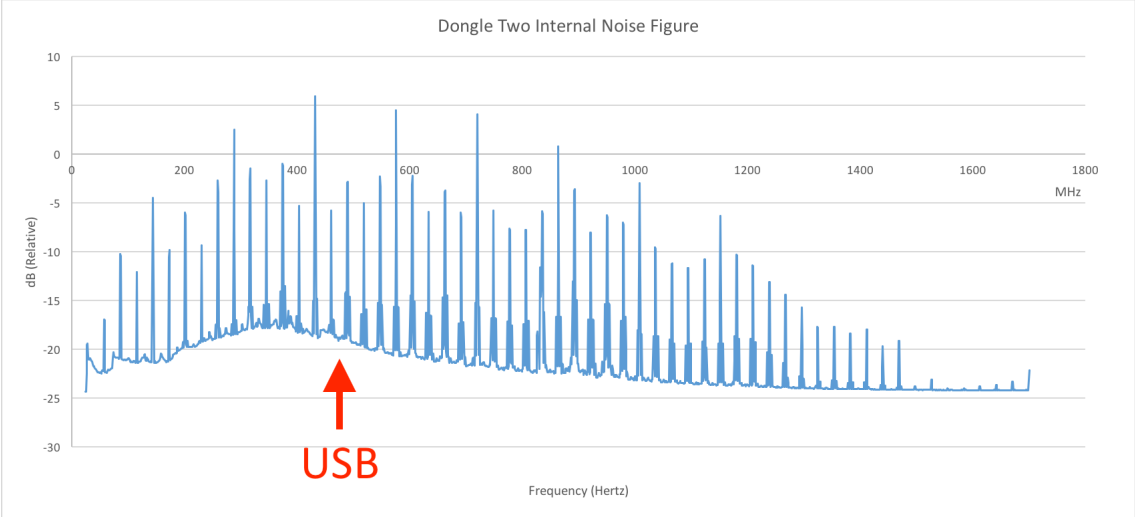


Figure 5.12: Modified RTL-SDR Dongle Internal Noise Figure: Dongle Two.

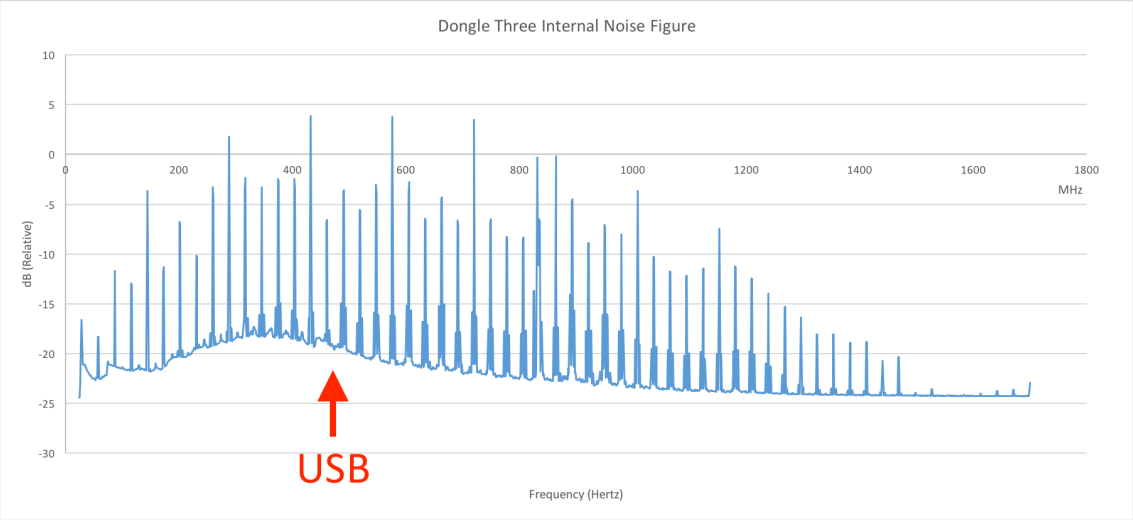


Figure 5.13: Modified RTL-SDR Dongle Internal Noise Figure: Dongle Three.

All three noise figure plots effectively represent the same image, this is a positive result, as it shows that all three hardware devices are equivalent, with sufficiently similar specifications. A distinctly different result from one or more of the dongles would represent an anomaly, and would alter the expected result.

The repetitive peaks present in each figure represent 28.8 MHz overtones that occur as a result of the external timing source generator. Whilst these overtones are consistent with an unmodified dongle, as shown by (Keen 2008), the amplitude of the overtones are relatively greater in magnitude due to the 10 mA supply from the Si5351 external clock generator. The large bump present at approximately 480 MHz is produced as a direct result of the USB data rate of 480 Mbps, with the overall width of the bump occurring due to USB bandwidth modulation.

The presented overtones do no represent a significant reduction in the capability of the receiver, so long as the frequency of interest does not occur at the same location as the overtone. An alternative option to reduce the impediment caused by the timing signal overtones, is to reduce the drive power of the Si5351 clock generator from 10 mA to its

minimum value of 2 mA. This modification requires a different Arduino code library to be implemented that is compatible with the power reduction capability of the VCO. The Adafruit Si5351 library does not support any reduction in the output drive level of the VCO.

5.7 Radio Receiver Band Scan

Section 3.4.5 identifies that to determine the suitability of any testing location, it is necessary to verify the strength of signals present in the range of interest at that location by conducting a scan over the relevant range of receiver frequencies, to view the relative power levels of all available signals. This test was undertaken using the RTL-Power application provided as a part of the modified Osmocom RTL2832U driver set (Osmocom 2016), for using the devices as a SDR. The data from each band was collected over 15 minutes and is presented in Figures 5.14 to 5.19. The RF bands of interest scanned were:

- Band II: 87.5 MHz to 108 MHz
- Band III: 174 MHz to 240 MHz
- Band IV: 470 MHz to 582 MHz

For each scanned band of interest, the traditional waterfall diagram was provided in conjunction with a 2D relative power diagram, which is more suitable for comparison to the relative noise diagrams presented in Section 5.6. Results were collected similarly to those for the noise testing, with an integration interval of 1 second, a gain of 50 dB, and a total scan time of 15 minutes. Longer scanning time will provide a more realistic picture of sporadic transmissions, however the focus of this research is commercial media transmitters, hence they will be present equally in a scan of any duration.

Figures 5.14 and 5.15 show the results of a scan conducted over Band II, the commercial FM radio band. Figure 5.14 is a waterfall diagram, showing signal intensity over the band on the X-axis, and how that changes over time on the Y-axis. The test presented in the figure is not discernible, however, it identifies the frequency range of the scan, the time, and the duration. Figure 5.15 shows the strength of signals over the band, with the Y-axis representing the power level of each signal in dB relative to the other signals present.

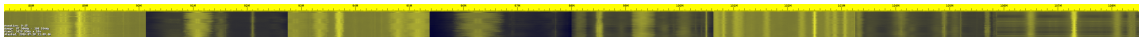


Figure 5.14: Radio Frequency Spectrum Band II Scan Waterfall Diagram.

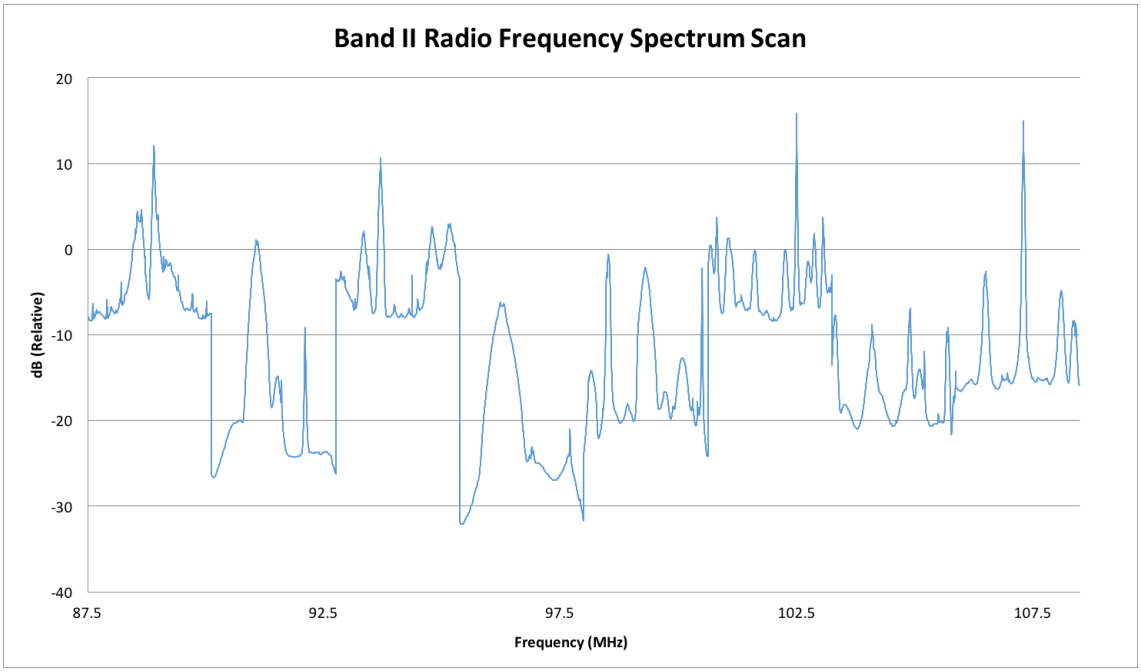


Figure 5.15: Radio Frequency Spectrum Band II Scan Relative Power (dB) Diagram.

Figures 5.16 and 5.17 show the results of a scan conducted over Band III, the lower region of the commercial TV band. Figure 5.16 is a waterfall diagram, showing signal intensity over the band on the X-axis, and how that changes over time on the Y-axis. The test presented in the figure is not discernible, however, it identifies the frequency

range of the scan, the time, and the duration. Figure 5.17 shows the strength of signals over the band, with the Y-axis representing the power level of each signal in dB relative to the other signals present.

Figure 5.16: Radio Frequency Spectrum Band III Scan Waterfall Diagram.

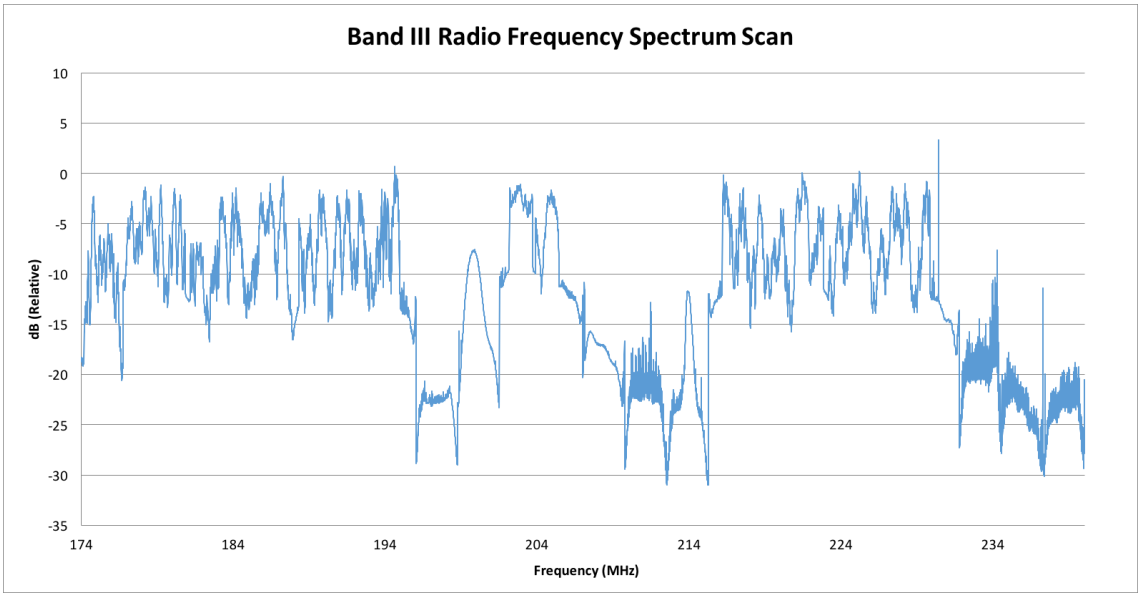


Figure 5.17: Radio Frequency Spectrum Band III Scan Relative Power (dB) Diagram.

Figures 5.18 and 5.19 show the results of a scan conducted over Band IV, the upper region of the commercial TV band. Figure 5.18 is a waterfall diagram, showing signal intensity over the band on the X-axis, and how that changes over time on the Y-axis. The test presented in the figure is not discernible, however, it identifies the frequency range of the scan, the time, and the duration. Figure 5.19 shows the strength of signals over the band, with the Y-axis representing the power level of each signal in dB relative to the other signals present.

Figure 5.18: Radio Frequency Spectrum Band IV Scan Waterfall Diagram.

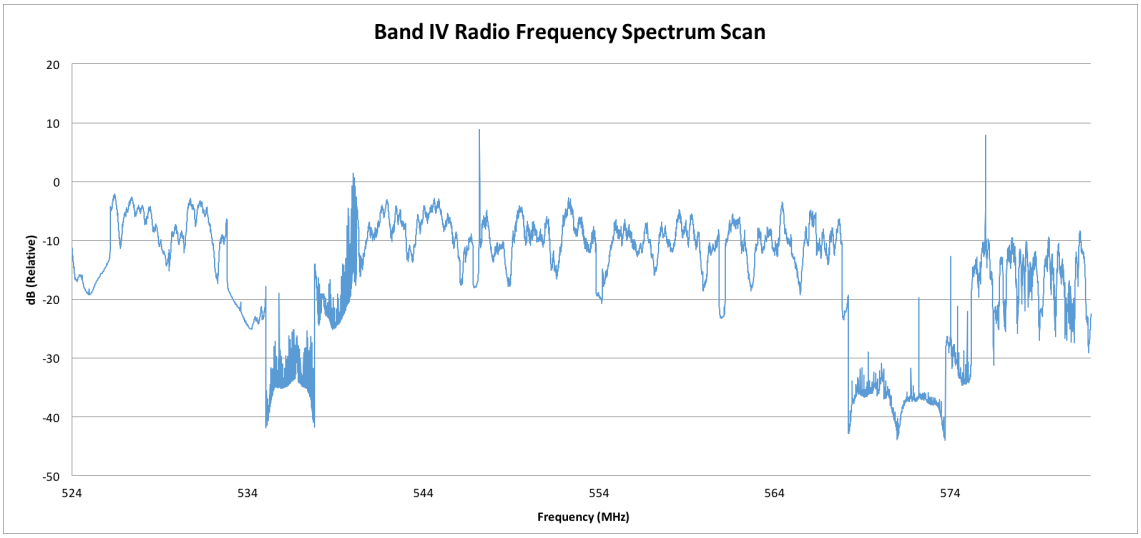


Figure 5.19: Radio Frequency Spectrum Band IV Scan Relative Power (dB) Diagram.

The results of the conducted band scans show that there are a multitude of sources of interest present across each band. There are at least 55 identifiable FM broadcast transmitters available, and although less visible due to their 7 MHz bandwidth, and their psuedo-random noise appearance, there are at least ten (10) identifiable TV transmitter signals contained within the scans of bands III and IV. It must also be noted that each band scan was conducted with an equal gain to that of the noise floor testing in Section 5.6, however the 28.8 MHz overtones that dominated the noise testing are much less significant with a suitable antenna attached, and signals of interest present. The 480 MHz lump is still present due to data rate of USB, this interference however, produces a negligible effect on any results.

5.8 Continuous Wave RADAR Test Software Evaluation

To validate the software implementation described in Section 4.16 for a low cost software defined radio passive RADAR, it was necessary to test its function with a known dataset. This was conducted with the software defined GNU Radio based Doppler RADAR described in Section 4.11. A frequency of 10 kHz was used in conjuction with the internal microphone of the test computer to simulate a basic monostatic Doppler RADAR. The intention of the test was to confirm the operation of the complex ambiguity function described in Section 2.2.4 and validate the implemented method of data windowing, hence verifying that the developed software implementation was suitable for use on the more complex modulated signal types that were the subject of this research.

A total of 240 data windows were calculated in the complex ambiguity function, representing one minute of data. Each window represents a $\frac{1}{4}$ second window, at a sampling frequency of 48 kHz, and therefore 12 000 samples per window. The sample cross-correlation variation across the dataset was 0, therefore, between the reference signal, and the surveillance signal, a perfect alignment between data sources was achieved. This alignment ensures that any deviation in frequency is representative of a Doppler shift, and not the result of a misalignment between the reference and surveillance signals.

From Equation 2.6 it can be expected that for a frequency of 10 kHz and human movement of approximately 5 m/s, there will be a Doppler shift, which will be represented in the results of the complex ambiguity function. As the test generator used was producing only a single frequency continuous wave output, there will be no time deviation, and therefore no possible range calculation. As a result of this, all result data from this test will display only the result of any Doppler shift.

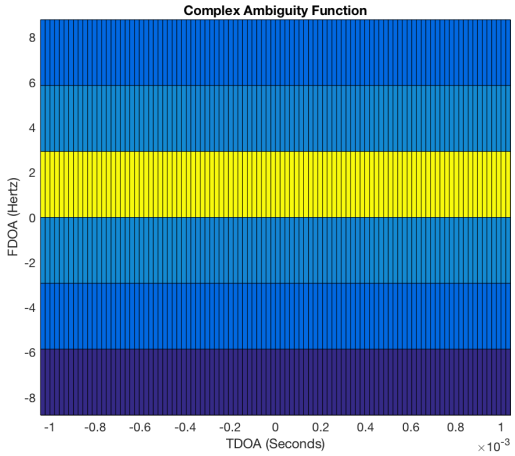


Figure 5.20: Software Implementation Evaluation Autocorrelation Reference Plot.

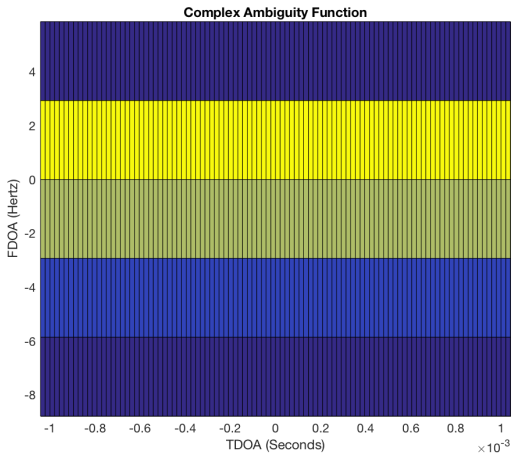


Figure 5.21: Software Implementation Evaluation Doppler Shift Plot.

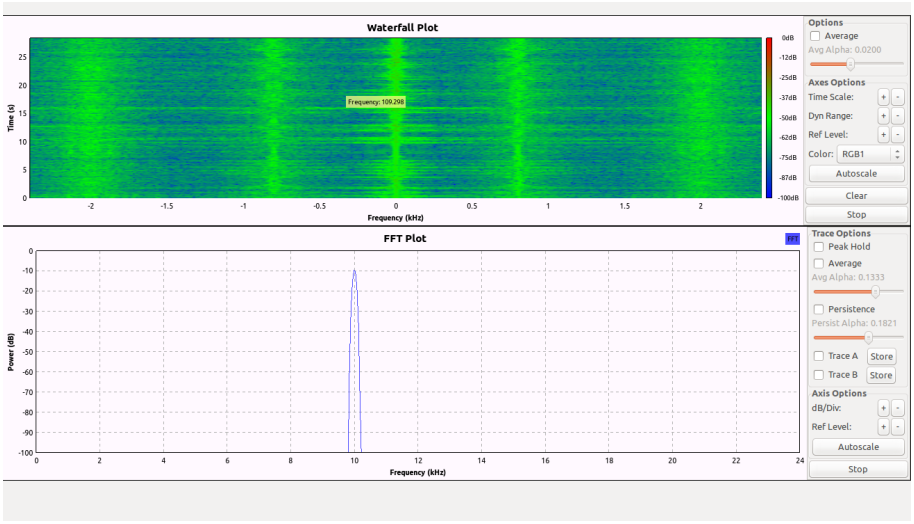


Figure 5.22: Software Implementation Evaluation Reference Display Data.

An autocorrelation of the reference signal, shown in Figure 5.20 identifies no recognisable Doppler shift. By comparison, Figure 5.21 depicts the Doppler shift over the same data window when the reference signal is correlated with the surveillance signal. The shift is represented by the movement of the yellow line from the reference position noted in Figure 5.20, depicts a Doppler shift of between 0 and 2 Hz. This result validates the operation of the developed hardware and software model. A similar result would be obtained for the autocorrelation of the surveillance signal, however, this has been omitted. This can be further confirmed by the output data generated by the program used, shown at Appendix I, and shown in Figure 5.22 whereby the expected Doppler deviation is represented graphically.

5.9 Continuous Wave RADAR Test Hardware Evaluation

To validate the hardware configuration described in Section 4.6 for a low cost software defined radio passive RADAR, it was necessary to verify its functionality in a controlled

environment. This was conducted with the Arduino based 433 MHz continuous wave transmitter described in Section 4.9. The transmitter was configured at a distance of 5 M from the coherent receiver, and a similar elevation. With the transmitter emitting, data was recorded in GNU Radio using the Multi-RTL module described in Section 4.12 and shown in Appendix J. The intention of the test was to confirm the operation of RTL2832U based software defined radio receivers as a passive bistatic RADAR receiver as described in Section 2.5.3 and validate the hardware and software configuration that forms the basis of this research.

A total of 23 data windows were calculated in the complex ambiguity function, representing 5.75 seconds of data. Each window represents a $\frac{1}{4}$ second window, at a sampling frequency of 500 kHz, and therefore 125 0000 samples per window. The sample cross-correlation variation across the dataset was 0.

From Equation 2.7 it can be expected that for a frequency of 433 MHz and human movement of approximately 5 m/s, there will be a visible Doppler shift, which will be represented in the results of the complex ambiguity function. As the test generator used was producing only a single frequency continuous wave output, there will be no time deviation, and therefore no possible range calculation. As a result of this, all result data from this test will display only the result of any Doppler shift.

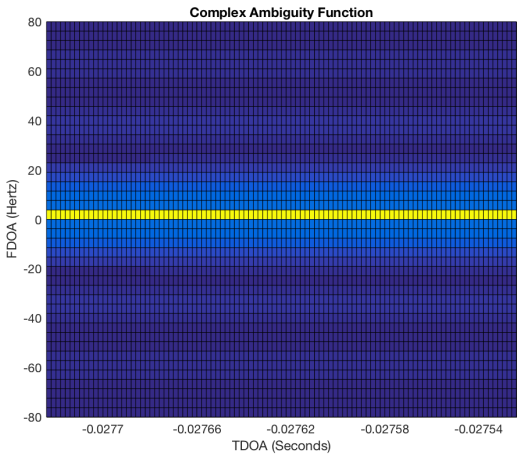


Figure 5.23: Software Implementation Evaluation Autocorrelation Reference Plot.

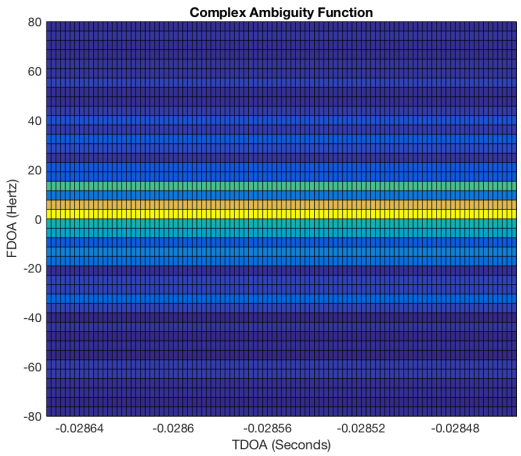


Figure 5.24: Software Implementation Evaluation Doppler Shift Plot.

An autocorrelation of the reference signal, shown in Figure 5.23 identifies no recognisable Doppler shift. By comparison, Figure 5.24 depicts the Doppler shift over the same data window when the reference signal is correlated with the surveillance signal. The shift is represented by the movement of the yellow line from the reference position noted in Figure 5.23, depicts a Doppler shift of between 0 and 20 Hz. This result validates the operation of the developed hardware and software model. A similar result would

be obtained for the autocorrelation of the surveillance signal, however, this has been omitted.

This test implementation has validated the operation of the developed RTL-SDR based passive RADAR receiver hardware, and confirmed the operation of the implemented software model, thus confirming that RTL-SDR based software defined radio receivers are capable of acting as passive bistatic RADAR receivers.

5.10 Passive Bistatic RADAR Data Collection - Location Overview

A survey was undertaken in the data collection location with a complete hardware configuration as outlined thoroughout this research. The intention of the survey was to determine the suitability of the location for the collection of data to produce a passive bistatic RADAR output. Data collection was conducted in stages to ensure suitability. Figure 5.25 shows the hardware configuration implemented for testing. Additionally, Figure 5.26 shows the antenna configuration implemented for testing, based on the implementation undertaken by McKay-Bukowski et al. (2015) where two log periodic antennas were co-located and capable of receiving passive bistatic RADAR data with a similar hardware configuration using FM modulated signals.

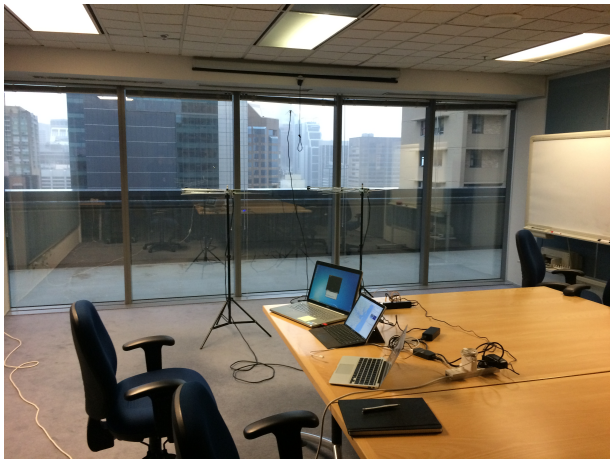


Figure 5.25: Passive Bistatic RADAR Data Collection Equipment Configuration.

Figure 5.26: Passive Bistatic RADAR Data Collection Antenna Configuration.

A scan identifying television channel frequencies available at a strength sufficient to enable regular viewing was undertaken, with the available options presented in Table 5.1.

Frequency (MHz)	Polarisation	Station	Location	Callsign
177.50	Horizontal	Seven	Willoughby/Artarmon	ATN6
184.50	Horizontal	SBS	Gore Hill/Artarmon	SBS7
191.625	Horizontal	Nine	Willoughby/Artarmon	TCN8
219.50	Horizontal	Ten	Willoughby/Artarmon	TEN11
226.50	Horizontal	ABC	Gore Hill/Artarmon	ABC12
529.50	Horizontal	Seven	Manly	ATN28
543.625	Horizontal	ABC	Manly	ABC30
550.50	Horizontal	Ten	Manly	TEN31
557.50	Horizontal	SBS	Manly	SBS32
564.50	Horizontal	Nine	Manly	TCN33

Table 5.1: Data Collection Location DVB-T Frequency Availability Data.

The conducted scan identified ten (10) unique DVB-T transmissions, plus a substantial number of FM radio stations, and DAB+ radio stations that were suitable for use as non-cooperative passive bistatic RADAR transmitters.

The data in Table 5.1 was collected using the generic software provided with the dongles on purchase. As identified in Section 2.4.2, DVB-T processing is undertaken on-chip within RTL-SDR dongles. On-chip processing means that the full 7 MHz bandwidth of the received channel is not passed through the USB data stream, but a decoded data stream is. The main limitation observed with RTL-SDR dongles is that the in-phase and quadrature data stream, primarily used by the SDR drivers, is limited to a maximum bandwidth of 3.2 Msps, and a stable maximum of 2.4Msps. This data rate is substanitally less than that required to process a full DVB-T signal, hence SDR# and GQRX were not suitable for identifying the available and tunable TV networks.

Location	Carriers	Power (kW)	Antenna Pattern	Coordinates (Lat, Long)	Elevation (M)	Tx Height (M)
Artarmon	5	50	Omnidirectional	-33.81, 151.18	107	197
Gore Hill	2	50	Omnidirectional	-33.82, 151.19	95	158
Manly	5	1	Omnidirectional	-33.81, 151.30	77	51
Willoughby	3	50	Omnidirectional	-33.81, 151.19	77	223

Table 5.2: Data Collection Location: Visible Transmitter Sites.

From the identified signals in Table 4.3, a subsequent number of transmitter locations were identified. Table 5.2 contains a breakdown of the details for each available transmitter location.

The data identifies that aside from a small repeating transmitter, which radiates at a substantially reduced power level in comparison to the other transmitters, the remaining three (3) locations are near enough to each other to be considered co-located. With the assumption of co-location, the diagram shown in Figure 5.27 was produced to identify the geographical relationship between the transmitter site, the receiver site, and the location of potential targets, based upon a known flight path.

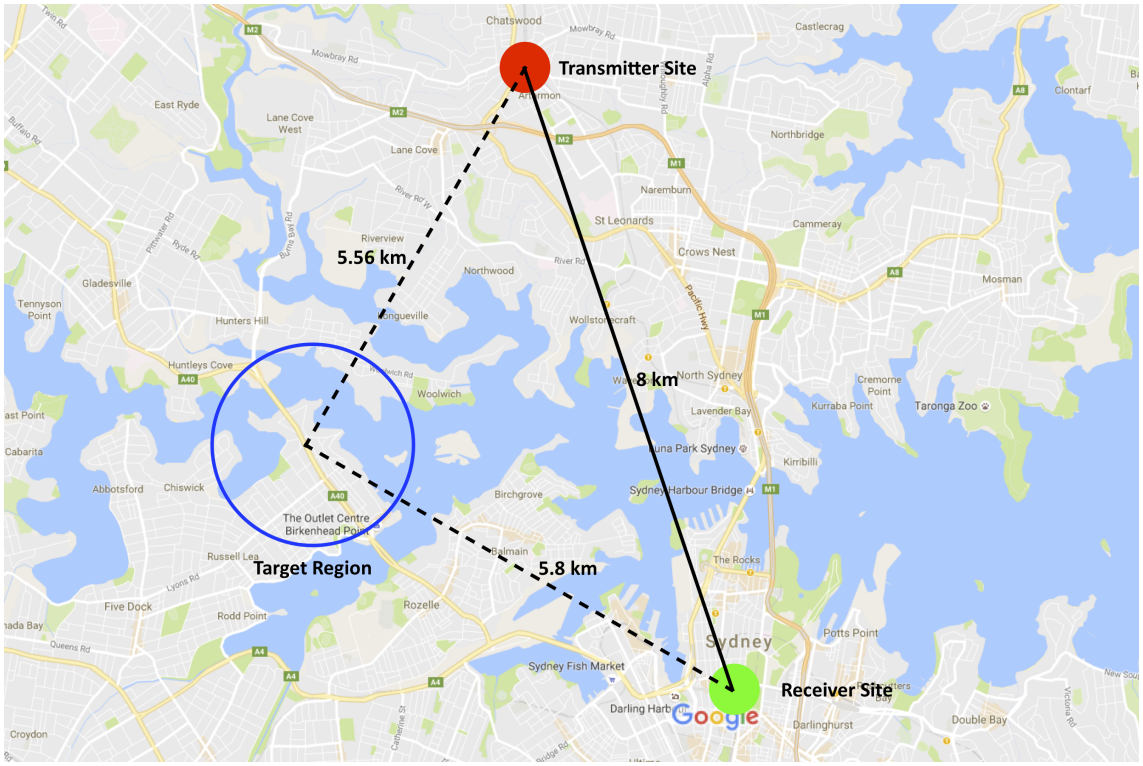


Figure 5.27: Passive Bistatic RADAR Data Collection Geography.

The geographical representation in Figure 5.27 identifies an 8 km distance between the transmitter and receiver. Using Equation 2.8, it has been calculated that the reference signal took 26.67 μS from transmission to reception over this path. Based on the target location of interest, from Equation 2.8, it has been calculated that the time for a signal to reach a target in the centre of the target area was 18.53 μS, and subsequently, the time for the reflected signal to reach the receiver was 19.34 μS giving a surveillance signal total time of 37.6 μS. This results in a difference of approximately 11 μS. The delay time was calculated independently of the frequency and type of modulation and is based on the speed of light in a vacuum. Noting that the calculation has been made for the centre of the denoted area of interest, there will be variance, however this calculation was provided to determine an approximate range of interest, hence providing an expected output.

The location used to collect data for this research has a Northerly aspect, hence, to achieve suitable gain, it is preferred that the air traffic being used as a RADAR target should also approach from the north, to position it within the area of interest identified in Figure 5.27. This favourable aircraft position, whilst presenting a stronger reflection position, also provides a considerable set of negative properties. Prevailing conditions in Sydney present wind from the north, hence, the majority of air traffic in regular conditions will arrive at runway 16, that being the northerly facing runway with an approach bearing of 160°. For aircraft to pass through the area of interest identified, and land on runway 34, representing a northerly approach with a runway bearing of 340°, conditions require a southerly wind, which brings conditions that are less than favourable for RADAR propagation. Generally, a southerly wind will occur with cloud, rain, and low visibility. Cloud and rain introduce a phenomenon known as backscatter, whereby RADAR range is reduced and/or confused by reflections from the increased water particles in the air. On the day that data was collected for this research, these less than favourable conditions were present; visibility was reduced to between 1 km and 6 km, and although there was no way to definitively measure, it is expected that the conditions will have had an impact on the result achievable. Figure 5.28 was produced during the data collection process and is representative of the conditions incurred throughout.

Figure 5.28: Graphical Representation of the Weather Conditions Under Which Data was Acquired.

5.11 Passive Bistatic RADAR Data Collection - FM Radio Transmitter

The initial test conducted was on an FM radio frequency of 104.9 MHz as the station plays predominantly rock music, which, as identified by Bezousek & Schejbal (2008) provides the best modulation rate for passive bistatic RADAR. This test was undertaken to verify the work conducted by McKay-Bukowski et al. (2015). As their work was largely undocumented, implementation was based on the research shown in Chapter 2 and the methodology defined in Chapter 3. To verify the capability of the processing software described in Sections 4.12 and 4.16 data collection occurred over two sample rates, both 1 Msps and 2 Msps. The different bandwidth implementations were possible with FM radio as it has a sufficiently small bandwidth to fit within either sample rate.

The data collected at 1 Msps was based around an aircraft target identified in Figure 5.29. A total of 60 seconds of data was collected and divided into 240 windows. Windows were $\frac{1}{4}$ second, as has been consistently used throughout this research. Each window contains 250 000 integrated samples, and a cross correlation of ± 1 sample was achieved consistently throughout data acquisition.

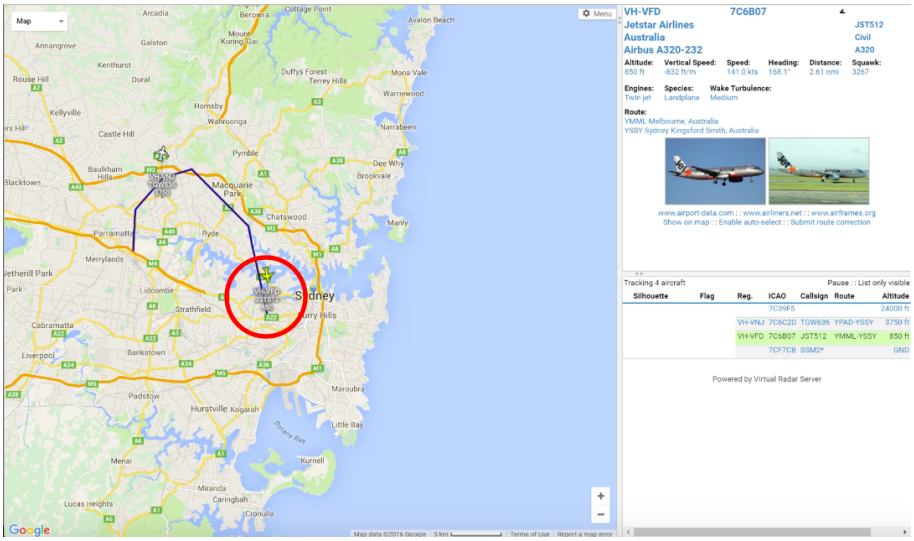


Figure 5.29: RADAR Reference Receiver Target Identification for FM Radio Data Acquisition at 1 Msps, Showing the Target (Red Circle) and Trajectory (Blue Line).

The data collected was analysed with the complex ambiguity function through MATLAB as described in Section 4.16, limited results were produced, with no data window providing a result that was clear enough to confirm successful target identification. Figure 5.30 shows a representative image of what was present in the majority of data samples collected. The large spike in the centre represents an exact correlation, with a time shift of 0, and a doppler frequency shift of 0, hence there is no target identified.

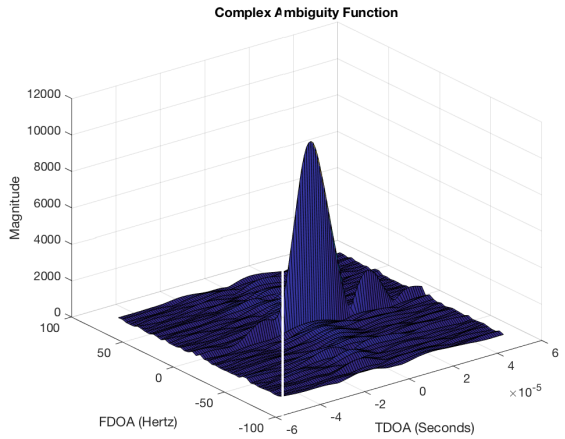


Figure 5.30: Passive Bistatic RADAR Complex Ambiguity Function Target Identification Result for FM Input at 1 Msps.

A small number of windows contained both a time and frequency shift, representing the identification of a target, however, the signal present does not align with the delay expected from Section 5.10 and does not confer with the results of Equation 2.7, hence it can be established that the target identified was not the aircraft of interest, but another target, this result can be seen in Figure 5.31. Without suitable data covering the full RADAR range, it is not possible to identify the target, or confirm that the result represents a target, or noise.

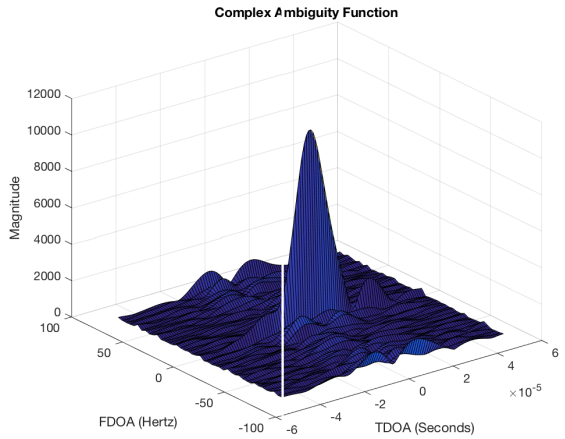


Figure 5.31: Passive Bistatic RADAR Complex Ambiguity Function Target Identification Result for FM Input at 1 Msps With Target Variation.

The data collected at 2 Msps was based around an aircraft target identified in Figure 5.32. A total of 15.5 seconds of data was collected and divided into 62 windows. Windows were $\frac{1}{4}$ second, as has been consistently used throughout this research. Each window contains 500 000 integrated samples, and a cross correlation of ± 1 sample was achieved consistently throughout data acquisition. The reduced length of the sample data was a result of the collection program stability. At the sample rate under test, the program cannot maintain coherence in the same manner as was achieved at 1 Msps.

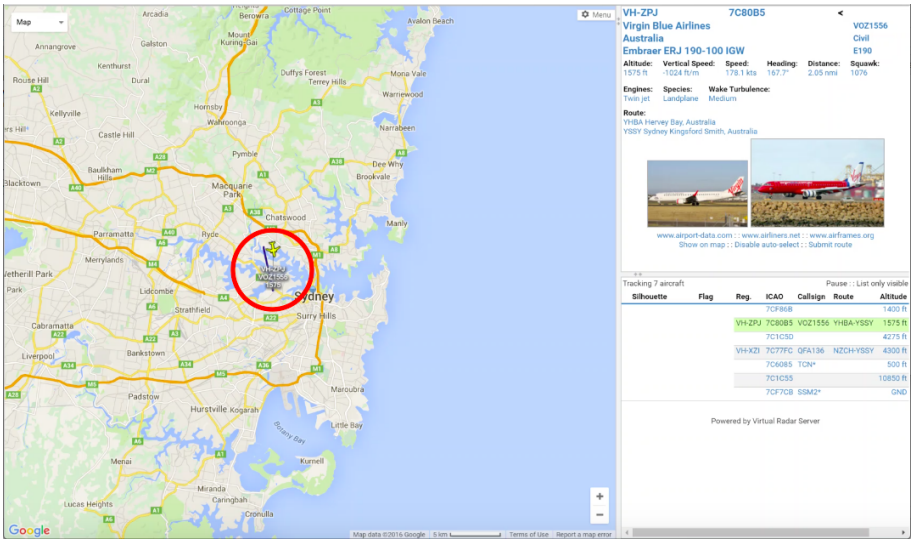


Figure 5.32: RADAR Reference Receiver Target Identification for FM Radio Data Acquisition at 2 Msps, Showing the Target (Red Circle) and Trajectory (Blue Line).

The data collected was analysed with the complex ambiguity function through MATLAB as described in Section 4.16, limited results were produced, with no data window providing a result that was clear enough to confirm successful target identification. Figure 5.33 shows a representative image of what was present in the majority of data samples collected. The large spike in the centre represents an exact correlation, with a time shift of 0, and a doppler frequency shift of 0. The symmetrical spikes produced at $\pm$ 60 Hz and a delay of 1 μS are not identifiable and are assumed to be noise, hence there is no target identified.

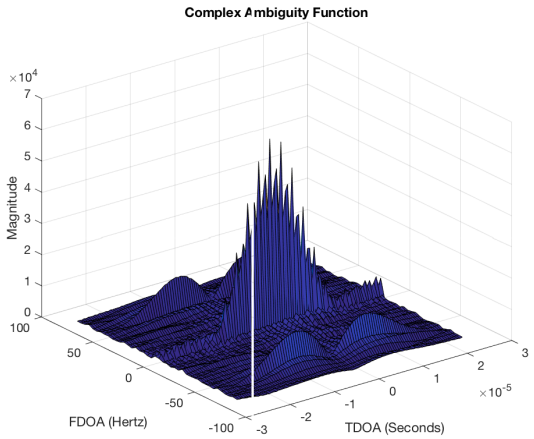


Figure 5.33: Passive Bistatic RADAR Complex Ambiguity Function Target Identification Result for FM Input at 2 Msps.

5.12 Passive Bistatic RADAR Data Collection - DAB+ Radio Transmitter

The second sample collection test conducted was on a DAB+ radio frequency of 209.928 MHz. This test was undertaken to verify the work conducted by Silverwood (2014). As his work was undocumented, implementation was based on the research shown in Chapter 2 and the methodology defined in Chapter 3. To verify the capability of the processing software described in Sections 4.12 and 4.16 data collection occurred at 2 Msps.

The data collected was based around an aircraft target identified in Figure 5.34. A total of 2.25 seconds of data was collected, due to repeated issues with maintaining coherence between the two receivers. The data was subsequently divided into 9 windows. Windows were $\frac{1}{4}$ second, as has been consistently used throughout this research. Each window contains 500 000 integrated samples, and a cross correlation of ± 1 sample was achieved consistently throughout data acquisition over the samples available.

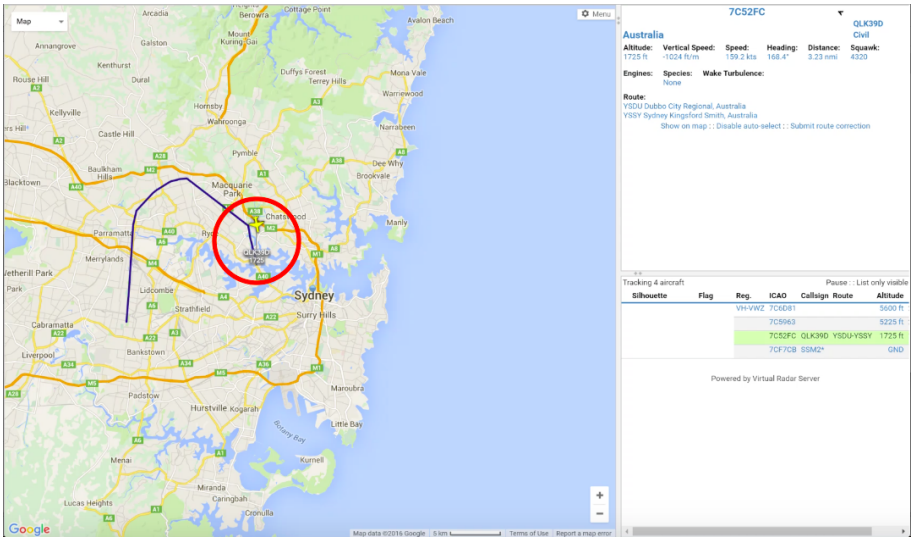


Figure 5.34: RADAR Reference Receiver Target Identification for DAB+ Radio Data Acquisition, Showing the Target (Red Circle) and Trajectory (Blue Line).

The data collected was analysed with the complex ambiguity function through MATLAB as described in Section 4.16, limited results were produced, with no data window providing a result that was clear enough to confirm successful target identification. Figure 5.35 shows a representative image of what was present in the majority of data samples collected. The large spike in the centre represents an exact correlation, with a time shift of 0, and a doppler frequency shift of 0, hence there is no target identified.

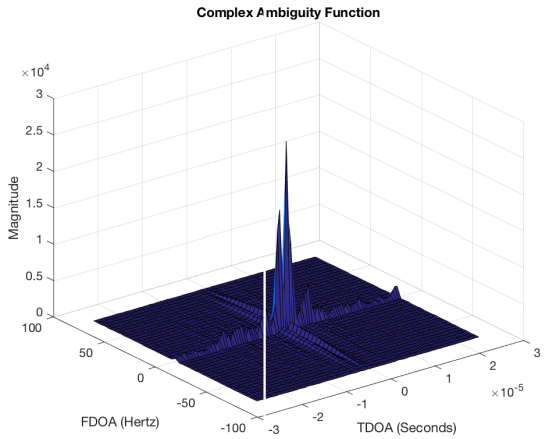


Figure 5.35: Passive Bistatic RADAR Complex Ambiguity Function Target Identification Result for DAB+ Input.

5.13 Passive Bistatic RADAR Data Collection - DVB-T TV Transmitter

The third sample collection test conducted was on a DVB-T television frequency of 177.5 MHz. This test was undertaken to satistfy the project objectives, determine whether RTL-SDR dongles are capable of acquiring passive bistatic RADAR data. Implementation was based on the research shown in Chapter 2 and the methodology defined in Chapter 3. To verify the capability of the processing software described in Sections 4.12 and 4.16, data collection occurred at 2 Msps.

The data collected at 2 Msps was based around an aircraft target identified in Figure 5.36. A total of 32.25 seconds of data was collected, due to repeated issues with maintaining coherence between the two receivers. The data was subsequently divided into 129 windows. Windows were $\frac{1}{4}$ second, as has been consistently used throughout this research. Each window contains 500 000 integrated samples, and a cross correlation of ± 1 sample was achieved consistently throughout data acquisition over the samples available.

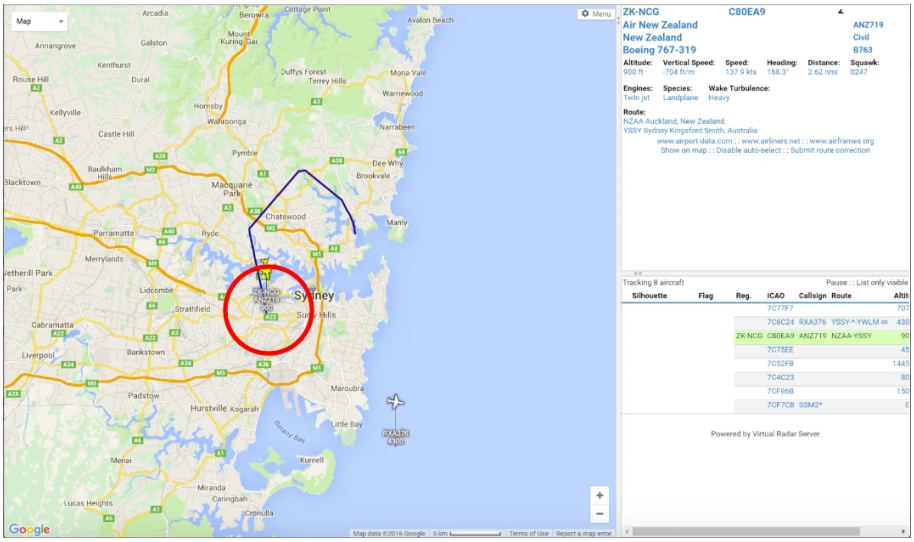


Figure 5.36: RADAR Reference Receiver Target Identification for DVB-T Television Data Acquisition, Showing the Target (Red Circle) and Trajectory (Blue Line).

The data collected was analysed with the complex ambiguity function through MATLAB as described in Section 4.16, limited results were produced, with no data window providing a result that was clear enough to confirm successful target identification. Figure 5.37 shows a representative image of what was present in the majority of data samples collected. The large spike in the centre represents an exact correlation, with a time shift of 0, and a doppler frequency shift of 0, hence there is no target identified.

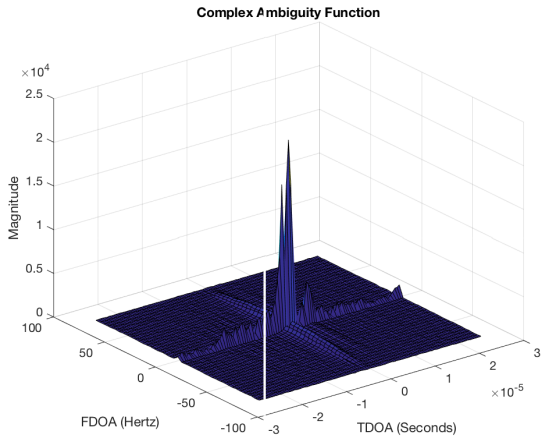


Figure 5.37: Passive Bistatic RADAR Complex Ambiguity Function Target Identification Result for DVB-T Input.

5.14 Discussion

The results presented in this chapter outline the results of testing undertaken to determine the suitability of RTL-SDR dongles as passive bistatic RADAR receivers. The results have confirmed that the internal clock used on RTL-SDR dongles is inadequate to provide coherent and stable passive RADAR data for processing, the external clock source detailed in Section 4.4 rectifies this problem, and produces a more stable result. The modified hardware was confirmed to function equally following modification, and the noise characteristics of the modified hardware have been presented. Results validating the software and hardware implementations have been presented, and a functional test carried out in an uncontrolled environment.

The results presented in Section 5.3 identify a large variation in clock frequency within a one hour period, this variation is outside the maximum requirement for the RTL2832U chipset to stream uninterrupted data to a computer, hence dropped samples will occur,

resulting in a lack of coherence. This confirms that the use of a shared crystal, as presented in Section 2.4.3.1, would still result in an unsuitable level of coherence between the reference signal and surveillance signal.

The external clock generation method presented in Section 4.4 has been tested to verify that it is within a suitable tolerance band to enable coherent sampling with multiple receivers. The operation of the devices has been benchmarked against the operation of an unmodified device and confirmed to be of equal function. The performance of the modified devices was then tested to determine their suitability for passive RADAR reception. Based on the results achieved, the receiver has a suitable level of discrimination above the noise floor in which reflected target data can be collected. A subsequent scan of the bandwidth intended to be monitored for target signals identified a number of potential non-cooperative targets, and subsequently verified that these carriers exceeded the noise magnitude of the hardware.

A test of the implemented software solution verified its capability to discern doppler shift, and hence verified the suitability of the implementation for passive RADAR data processing. This test was repeated using a hardware transmitter and coherently configured RTL-SDR receivers, thus verifying that the developed hardware configuration was also capable of receiving, and subsequently processing and identifying doppler shift where movement had occurred. This testing confirmed that the hardware configuration developed in Chapter 4 is capable of functioning as a passive bistatic RADAR receiver. The subsequent testing identified the capability of the receiver when used with the non-cooperative signals available in the test region.

A factor for consideration in the achieved results is the polarisation of the antennas. By design, the log periodic antennas used will only receive horizontally polarised signals. This was confirmed when an additional test was conducted using the provided antenna shown in Figure 4.13, where, under a generic TV Tuner software test, vertically polarised signals from regional transmitters were successfully identified. This horizontal polari-

sation limitation means that if a signal reflected from the target of interest changes in polarity when it reflects, the implemented antenna under test will not successfully receive that reflection, and the target will be missed.

Section 4.14 identified a number of security implications for civilian capture of passive RADAR data. The geography of the location was a primary concern, with relative proximity to targets, and being within a suitable range of the transmitter, to ensure received signals are of suitable strength. With the geographical limitations described, a location within 10 km of the Sydney central business district was required, providing access to both transmitter towers at a suitable relative power, and access to a flight path where targets could be found, Section 4.14 subsequently identified that any location would need to be on private property, with permission granted by the property manager. This limitation applies due to the current level of perceived security threat to the public, it was anticipated that the RADAR hardware configuration required, if used in a public space, such as a park, would generate fear and would cause unwanted attention.

From the defined location requirements, a suitable location was sourced with a northerly aspect, thus requiring airborne targets to be landing on runway 34 and having a north - south approach. Subsequently, for this to occur, conditions needed to be different to those generally prevailing, thus a southerly wind, which also produces cloud and therefore backscatter was an indirect byproduct of the available data collection location. These factors combine to reduce the likelihood of achieving confirmed target identification when processing the acquired data.

The data collected for FM radio broadcasts on 104.9 MHz did show evidence of variation, however the target or noise identified was not that of the intended target, nor was there any method of validating the deviation against another target, hence the result cannot be confirmed as a valid passive bistatic RADAR function. The bandwidth of an FM radio signal falls within the 2 MHz bandwidth channel available on the RTL-SDR dongle, so it is expected, that in a different location, with the correct conditions, a result from this

frequency is achievable, and that for an FM signal, the RTL-SDR dongle can be used as a passive bistatic RADAR receiver.

The data collected from the DAB+ transmitter source provided similar results to that of the FM transmitter. No target was identifiable, but as the data was collected under the same conditions for each transmitter source, it is expected that the location limitations and weather conditions impacted the result achievable. The greater noise reduction properties of an OFDM signal are however visible in the data collected, as can be seen in Figure 5.35. The bandwidth of the signal falls within the 2 MHz bandwidth of the RTL-SDR receiver dongle, therefore, given the appropriate conditions and location, collection of passive RADAR data from a DAB+ non-cooperative source should be possible.

The data collected from the DVB-T transmitter source was also inconclusive. This result was influenced by the data collection location, and the weather conditions, however, it is expected that the primary reason for the lack of target identification is due to the bandwidth limitations of the RTL-SDR receiver. As the receiver is only capable of a maximum 3.2 MHz bandwidth, and is more realistically limited to 2 MHz by the software processing algorithm, a 7 MHz DVB-T channel cannot be fully received.

The architecture of the RTL2832U chipset is such that for decoding TV signals, processing is undertaken on-board the chip, with the demodulated data passed over USB to the host computer for user viewing. When the device is used as an SDR dongle, processing is required to be undertaken by the host computer, hence the throughput of the chip for In-Phase (I) and Quadrature (Q) signals is limited. This limitation prevents a full 7 MHz bandwidth DVB-T channel being processed.

Subsequently, the design of OFDM modulation is such that it is able to reject noise well, hence, any reflected target signal will be cancelled out by the signal modulation. This effect can be identified in the result data shown in Figure 5.37, when compared to the result produced by an FM signal, it can be seen that there is almost no deviation in time or frequency from the zero reference. The combination of OFDM noise rejection

properties, and the limited throughput capability of RTL-SDR dongles means that for the partial channel received, any target reflections are nulled by the modulation method, and the edges of the channel, where it is most likely that data could be acquired, are not able to be captured.

The results achieved demonstrate that RTL-SDR dongles are capable, and have been confirmed to operate suitably as doppler passive bistatic RADAR receivers. Testing conducted on signals received from an FM radio transmitter were inconclusive, failing to identify the target of interest. This differs from the results presented by McKay-Bukowski et al. (2015), where a video has been presented showing passive RADAR targets identified through the use of an FM radio source. Similarly, the results achieved for testing conducted on a DAB+ source also proved inconclusive, failing to identify any target data, and differing from the result achieved by Silverwood (2014).

Testing conducted on the primary signal source of interest, DVB-T broadcast was not successful in identifying any targets throughout the testing process. Based upon the results achieved for FM transmitters, and DAB+ transmitters, which both differ from the undocumented results of the testing conducted by McKay-Bukowski et al. (2015) and Silverwood (2014) respectively, further testing in alternative locations is required to confirm the operation of RTL-SDR dongles as a passive RADAR with any FMCW source. Based on the results presented in this Section, and the input requirements for a passive inverse synthetic aperture RADAR defined in Sections 2.2.2.3 and 2.2.2.4, it can be concluded that RTL-SDR dongles are not suitable for use as a passive inverse synthetic aperture RADAR receiver.

5.15 Chapter Summary

This chapter has presented the results that were obtained from the passive bistatic RADAR system designed in Chapter 4. The results convey the functionality of the RTL-SDR platform prior to, and following modification, and detail the results of data collection and processing with RTL-SDR dongles configured to function as a passive bistatic RADAR receiver. The discussion summarises the results obtained, drawing conclusions on the functionality of the system both at a component level, and as a system.

6

Further Work

This chapter presents a compendium of research options available to expand the subject research and further develop Realtek RTL2832U chipset based devices as Passive Bistatic RADAR (PBR) receivers.

6.1 Introduction

Further work to be completed beyond the scope of the project includes identification of suitable alternative data collection locations, improvements to the receiver reliability, experimental evaluation of the results presented in this research, analysis and improvement of the receiver hardware to reduce the noise floor, and the addition of directivity to the received RADAR information.

6.2 Identification of Alternative Data Collection Locations

Due to the security implications identified in Section 4.14, the data available was limited, reducing the breadth of results data available. Identification of suitable alternative locations that fall within the security requirements, and are in a suitable location to collect data from a source that produces large reflections, such as aircraft or large ships, will enable a greater data set from which software processing and refinement can occur.

6.3 Modification to Achieve Consistent Results from FM and DAB+

In line with the previous section, with a greater data set, modification of the software and antenna configuration can be made to achieve consistent target identification from FM radio stations and DAB+ radio stations. Both of these identified sources fall within the maximum bandwidth limitations of RTL-SDR dongles, and, based on the results achieved, should be capable of producing passive bistatic RADAR data.

6.4 Confirm the Results Achieved With an Alternative Hardware Receiver

To confirm the results achieved in Chapter 5, concurrent data acquisition with the RTL-SDR passive RADAR receiver defined in Section 4.6 and one of the purpose built receivers described in Section 2.4.2, capable of a larger receiver bandwidth, should occur. By concurrently recording data, the results can be assumed to be coherent between receiver systems. Where a variation in the results, or, an identification of targets using DVB-T frequencies occurs on the dedicated hardware receiver, confirmation of the experimental results presented in this paper will occur.

6.5 Implement Software Improvements to Reduce Processing Delay

The main limitation with the implemented Passive Bistatic RADAR (PBR) is the processing delay, one data window can take up to 30 seconds to process, dependent on the sampling rate, and the number of samples present in the window. This result does not achieve a real time representation of the targets in any location. For a PBR to be useful, processing must occur at or near real time.

6.6 Implement Hardware Improvements to Reduce Noise Floor

The high noise floor present in RTL-SDR dongles can primarily be explained by device hardware configuration. It is common for the operating temperature of the dongle to reach in excess of 40°C, which is approaching the reliable operating limit of a number

of the internal components. Relocation of the onboard voltage regulators to an adjacent circuit board would reduce the primary heat source, and provide a larger area for additional cooling components to be fitted to the RTL2832U chip, and the 820T chip. Suitable enclosure design and a reduction in the external timing source generator supply current can also be implemented to reduce noise.

6.7 Add Additional Receivers to Provide Direction Data

The addition of an extra hardware receiver to the two extant in the current configuration will allow for direction data to be collected. Making use of a known north point, or through the integration of a Global Positioning System (GPS) receiver, it is possible to produce a more accurate representation of potential targets identified by the Passive Bistatic RADAR (PBR).

7

Conclusions and Recommendations

This chapter summarises the results achieved and compares these to the original project specification objectives. The strengths and weaknesses of assumptions and results are analysed and extrapolated into research that can be undertaken to improve knowledge in the subject.

7.1 Conclusions and Recommendations

This research has determined the suitability of a software defined radio passive bistatic RADAR receiver, having made use of hardware radio receivers based on the Realtek RTL2832U chipset. A review of existing developments in the field of passive bistatic RADAR has been conducted to determine an appropriate scope and realistic expectations of the hardware devices, a review of existing software developments was conducted to determine the most effective implementation, a review of existing developments in the use of digital television broadcasts to produce an inverse synthetic aperture RADAR image was conducted, and the hardware requirements of a passive bistatic RADAR based upon the Realtek RTL2832U chipset were determined and contrasted against other software defined radio receiver hardware.

This dissertation has determined the suitability of a low cost software defined radio receiver based upon the Realtek RTL2832U chipset as an interface for an Inverse Synthetic Aperture Passive Bistatic RADAR. Testing and evaluation has determined a suitable configuration of the hardware receiver, from which a software interface was then developed. The combined hardware and software platforms was tested in both controlled and uncontrolled environments to determine their overall suitability as a viable solution to the problem.

Research has been undertaken into bistatic passive RADAR systems and their implementation through software defined radio, the use of DVB-T broadcast signals to produce an ISAR output, and use of the Realtek RTL2832U TV tuner as an SDR receiver. The research found that existing implementations made use of purpose built hardware, that was expensive and beyond the reach of a hobbyist. Of the existing examples of passive bistatic RADAR through software defined radio, many used FM radio to identify targets, and some made use of DAB+ radio. Those that did use DVB-T were using purpose

built SDR hardware, and of that group, some were able to achieve an Inverse Synthetic Aperture RADAR (ISAR) output. The use of RTL2832U TV tuner based receivers for passive RADAR was implied in a selection of documentation, but the process by which a result was achieved was largely undocumented.

Development of test hardware to evaluate the suitability of the RTL28322u receiver for Inverse Synthetic Aperture RADAR (ISAR) Passive Bistatic RADAR (PBR) was undertaken, with the results identifying that the hardware is capable of capturing the requisite range and velocity information required to produce an Inverse Synthetic Aperture RADAR (ISAR) output.

Development and integration of a software solution to interface the receiver resulting in the production of a RAdio Detection And Ranging (RADAR) display was undertaken. The resulting display is capable of identifying doppler shift, from which velocity and a determination of arrival or departure can be calculated, and time deviation, from which the target range can be calculated.

Testing of the circuit and software in a controlled and real world environment was undertaken, making use of known reference signals to evaluate the performance of the hardware and software in controlled conditions, then validating the circuit with commercial radio sources. The results from testing identified that modified RTL2832U based receivers with suitable software processing are capable of receiving and displaying RADAR target information for doppler signals. Testing conducted on real world environment sources was unable to identify any target data, however possible reasons for this result have been provided.

Evaluation of the suitability of Realtek R2832u based receivers as the hardware receiver in a Passive Inverse Synthetic Aperture RADAR (PISAR) was undertaken. Based on the results achieved and the limited bandwidth capability of Realtek R2832u based receivers when transporting in-phase and quadrature data over a USB connection, it was identified that a full 7 MHz DVB-T channel could not be processed by the receiver. The nature of

OFDM signals, is that they are designed to cancel out noise within their band, hence, as a full DVB-T channel could not be interrogated, no valid range or velocity data could be extracted to input to an Inverse Synthetic Aperture RADAR (ISAR) processing algorithm. Based on this, it has been determined that Realtek R2832u based receivers are not suitable as a hardware receiver for inverse synthetic aperture passive bistatic RADAR. Exchanging the RTL-SDR receiver for an alternate SDR hardware receiver would produce positive target identification.

References

Adafruit (2016), 'Adafruit Si5351A clock generator breakout board - 8KHz to 160MHz', https://www.adafruit.com/product/2045. [Online; accessed March-2016].

Air Services Australia (2016), 'How ADS-B works', http://www.airservicesaustralia.com/projects/ads-b/how-ads-b-works/. [Online; accessed June-2016].

AirSpy (2016), 'SDR# downloads', http://airspy.com/download/. [Online; accessed March-2016].

Aloi, G., Loscr, V., Borgia, A., Natalizio, E., Costanzo, S., Pace, P., Massa, G. D. & Spadafora, F. (2011), 'Software defined radar: synchronisation issues and practical implementation', pp. 1–5.

Anker, P. (2016), 'Bistatic radar – telecom ABC', http://www.telecomabc.com/b/bistatic-radar.html. [Online; accessed March-2016].

Australian Radiation Protection and Nuclear Saftey Agency (2002), *Maximum Exposure Levels to Radiofrequency Fields — 3 kHz to 300 GHz*, Vol. Radiation Protection Series Publication No. 3, Australian Radiation Protection and Nuclear Saftey Agency, Sydney, NSW.

Bezousek, P. & Schejbal, V. (2008), 'Bistatic and multistatic radar systems', *Radio Engineering* **17**(3), 53–59.

Brown, J. (2013), *FM Airborne Passive Radar*, University College London (University of London).

Carrara, W., Goodman, R. & Majewski, R. (1995), *Spotlight synthetic aperture radar:*

signal processing algorithms, Artec House, Boston.

Cass, S. (2013), 'A $40 software-defined radio'.

Costanzo, S., Spadafora, F., Di Massa, G., Borgia, A., Costanzo, A., Aloi, G., Pace, P., Loscri, V. & Moreno, O. H. (2013), 'Potentialities of USRP-based software defined radar systems', *Progress In Electromagnetics Research B* .

Csete, A. (2016), 'GQRX SDR', http://gqrx.dk. [Online; accessed March-2016].

Ettus Research (2016*a*), 'USRP N200', https://www.ettus.com/product/details/UN200-KIT. [Online; accessed March-2016].

Ettus Research (2016*b*), 'USRP N200/N210 networked series', https://www.ettus.com/content/files/07495_Ettus_N200-210_DS_Flyer_HR.pdf.

European Telecommunications Standards Institute (2009), *Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television*, European Telecommunications Standards Institute, France.

Faulconbridge, R. I. (2002), *Radar fundamentals*, Argos Press, Canberra.

Federal Communications Commission (n.d.), *Section 15.247 of the Rules and Regulations of the US Federal Communications Commission (FCC)*, Vol. 47 CFR 15.247, Federal Communications Commission.

Felguera-Martin, D., Gonzalez-Partida, J. T., Almorox-Gonzalez, P., Burgos-Garcia, M. & Dorta-Naranjo, B. P. (2011), 'Interferometric inverse synthetic aperture radar experiment using an interferometric linear frequency modulated continuous wave millimetre-wave radar', *IET Radar, Sonar & Navigation* **5**(1), 39–47.

Forum, S. (2002), 'Base station system structure', http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-01-P-0006-V2_0_0_BaseStation_Systems.

pdf. [Online; accessed March-2016].

Franklin, J. W. (2010), 'Passive bistatic radar', www.cse.unt.edu/~rakl/john-proposal.ppt. [Online; accessed June-2016].

Free TV Australia (2014), 'Free TV Australia operational practice OP–71', http://www.freetv.com.au/media/Engineering/Free_TV_OP_71_Recommended_DVB_T_Transmitter%20_Modulator_Settings_Issue_1_December_2014.pdf. [Online; accessed March-2016].

Freeman, D. (2007), The silent sentry system, *in* 'AoC 5th Multinational Converence of Passive Covert Radar'.

GNURadio (2016*a*), 'GNU Radio', http://gnuradio.org. [Online; accessed March-2016].

GNURadio (2016*b*), 'A quick guide to hardware and GNU Radio', http://gnuradio.org/redmine/projects/gnuradio/wiki/Hardware#A-Quick-Guide-to-Hardware-and-GNU-Radio. [Online; accessed March-2016].

Great Scott Gadgets (2016), 'HackRF One', http://greatscottgadgets.com/hackrf/.

Group, T. (2010), 'The HA100 passive radar from thales to play a role in protecting the flypast on 14th july in Paris', http://www.thalesgroup.com/Pages/PressRelease.aspx?id=13287. [Online; accessed March-2016].

Gutierrez del Arroyo, J. R. (2012), Passive Synthetic Aperture Radar Imaging Using Commercial OFDM Communication Networks, Phd.

Heunis, S., Paichard, Y. & Inggs, M. (n.d.), Passive radar using a software-defined radio platform and opensource software tools, *in* '2011 IEEE RadarCon (RADAR)', pp. 879–884.

Hyde, P. (2015), 'Comparing the RTL2832 and FCD Pro Plus receivers for meteor scatter applications', *The RAGazine* **2**(4), 14–18.

Jetvision.de (2014), 'RTL-1090', http://rtl1090.web99.de. [Online; accessed February-2016].

Johnson, J. J. (2001), Implementing the cross ambiguity function and generating geometry-specific signals, Master's thesis, United States Naval Post Graduate School, Monterey, California.

Keen, K. (2008), 'RTL power: Basic scripting', http://kmkeen.com/rtl-power/. [Online; accessed May-2016].

Krysik, P. (2016), 'Multi-RTL', https://ptrkrysik.github.io. [Online; accessed June-2016].

Kumar, B., DeRemer, D. & Marshall, D. (2005), *An Illustrated Dictionary of Aviation*, McGraw-Hill Education.

Kuschel, H. & O'Hagan, D. (n.d.), Passive radar from history to future, *in* 'Radar Symposium (IRS)', Vol. 2010 11th International, pp. 1–4.

Lackey, J. (2010), 'Kalibrate', https://web.archive.org/web/20131226204943/http://thre.at/kalibrate/. [Online; accessed June-2016].

Leech, M. (2013), 'Phase-coherence experiments with RTLSDR dongles', https://groups.google.com/forum/#\protect\kern-.1667em\relaxtopic/sara-list/02KyDILklRg. [Online; accessed March-2016].

Levanon, N. (n.d.), Multifrequency complementary phase-coded radar signal, *in* 'Radar, Sonar and Navigation', IEEE Proceedings, pp. 147(6):276–284.

Levanon, N. & Mozeson, E. (2004), *Radar Signals*, J. Wiley, Hoboken, NJ.

Liu, J., Li, H. & Himed, B. (2014), 'Two target detection algorithms for passive multistatic radar', *IEEE Transactions on Signal Processing* **62**(22), 5930–5939.

Mahafza, B. R. (2000), *Radar Systems Analysis and Design Using MATLAB*, Chapman & Hall/CRC, Huntsville, Alabama.

Markgraf, S. (2012), 'Kalibrate-RTL', https://github.com/steve-m/kalibrate-rtl. [Online; accessed May-2016].

Mathworks (2016*a*), 'MATLAB', http://au.mathworks.com. [Online; accessed March-2016].

Mathworks (2016*b*), 'RTL-SDR support from communications system toolbox', http://au.mathworks.com/hardware-support/rtl-sdr.html. [Online; accessed March-2016].

McKay-Bukowski, D., Vierinen, J., Virtanen, I. I., Fallows, R., Postila, M., Ulich, T., Wucknitz, O., Brentjens, M., Ebbendorf, N., Enell, C. F., Gerbers, M., Grit, T., Gruppen, P., Kero, A., Iinatti, T., Lehtinen, M., Meulman, H., Norden, M., Orisp, M., Raita, T., Reijer, J. P. d., Roininen, L., Schoenmakers, A., Stuurwold, K. & Turunen, E. (2015), 'KAIRA: the Kilpisjärvi Atmospheric Imaging Receiver Array – system overview and first results', *IEEE Transactions on Geoscience and Remote Sensing* **53**(3), 1440–1451.

Milldrum, J. (2016), 'Si5351 library for arduino', https://github.com/etherkit/Si5351Arduino. [Online; accessed March-2016].

Nuand (2016), 'BladeRF x40', https://www.nuand.com/blog/product/bladerf-x40/. [Online; accessed March-2016].

Olivadese, D., Giusti, E., Petri, D., Martorella, M., Capria, A., Berizzi, F. & Soleti, R. (n.d.), Passive ISAR imaging of ships by using DVB-T signals, *in* 'Radar Systems

(Radar 2012), IET International Conference on', pp. 1–4.

Olivadese, D., Martorella, M., Giusti, E., Petri, D. & Berizzi, F. (n.d.), Passive ISAR with DVB-T signal, *in* 'Synthetic Aperture Radar, 2012. EUSAR. 9th European Conference on', pp. 287–290.

Osmocom (2016), 'RTL-SDR', http://sdr.osmocom.org/trac/wiki/rtl-sdr. [Online; accessed March-2016].

Oxer, J. & Alexander, M. (2011), 'Freetronics leostick (arduino compatible)', http://www.freetronics.com.au/products/leostick#.V74-SFcwx5A. [Online; accessed August-2016].

Oxford English Dictionary (2016), *"radar, n."*, Oxford University Press.

Ozdemir, C. (2012), *Wiley Series in Microwave and Optical Engineering : Inverse Synthetic Aperture Radar Imaging With MATLAB Algorithms*, Wiley-Interscience, Hoboken, US.

Palmer, J. (2014), 'DSTO's passive radar research', http://www.ewh.ieee.org/r2/dayton/aess/meeting-documents/passive_radar_ieee_aes_hand.pdf. [Online; accessed May-2016].

Petri, D., Berizzi, F., Martorella, M., Mese, E. D. & Capria, A. (n.d.), A software defined UMTS passive radar demonstrator, *in* '11-th INTERNATIONAL RADAR SYMPOSIUM', pp. 1–4.

Petri, D., Capria, A., Conti, M., Berizzi, F., Martorella, M. & Dalle Mese, E. (2012), 'High-range resolution multichannel DVB-T passive radar: aerial target detection', *International Journal of Microwave and Wireless Technologies* **4**(02), 147–153.

Reis, A. L. G., Barros, A. F., Lenzi, K. G., Meloni, L. G. P. & Barbin, S. E. (2012),

'Introduction to the software-defined radio approach', *IEEE Latin America Transactions* **10**(1), 1156–1161.

Ridenour, L. N. (1947), *Radar system engineering*, Radiation Laboratory series, 1st edn, McGraw-Hill, New York.

RTL-SDR.com (2016*a*), 'Buy RTL-SDR dongles (RTL2832U)', http://www.rtl-sdr.com/buy-rtl-sdr-dvb-t-dongles/. [Online; accessed March-2016].

RTL-SDR.com (2016*b*), 'RTL-SDR', http://www.rtl-sdr.com.

Salsburg, J. (2015), 'Software defined radio', http://radar.salsburg.com/index.php?p=/discussion/4/software-defined-radio. [Online; accessed March-2016].

Schrödle, S. (2014), 'R820T, RTL2832U: SDR USB stick hack – clean and stable reference!', http://www.simonsdialogs.com/2014/09/r820t-rtl2832u-sdr-usb-stick-hack-clean-and-stable-reference/. [Online; accessed March-2016].

Silverwood, B. (2014), 'Low cost RTL-SDR passive multistatic DAB radar', https://www.youtube.com/watch?feature=player_embedded&v=l9V73d0nF4A. [Online; accessed March-2016].

Simpson, R. A. (1993), 'Spacecraft studies of planetary surfaces using bistatic radar', *IEEE Transactions on Geoscience and Remote Sensing* **31**(2), 465–482.

Standards Australia (1998), *Australian Standard AS2772.1: Radiofrequency Fields Part 1: Maximum exposure levels-3 kHz to 300 GHz*, Standards Australia, Sydney, NSW.

Standards Committee, L. (2002), *IEEE Standard for Local and Metropolitan Area Networks*.

Stevens, M. (1988), *Secondary Surveillance Radar*, Artech House.

Superkuh (2016), 'RTL-SDR and GNU Radio with Realtek RTL2832U [Elonics E4000/Raphael Micro R820T] software defined radio receivers.', http://superkuh.com/rtlsdr.html. [Online; accessed March-2016].

Szlachetko, B. & Lewandowski, A. (2012), 'A multichannel receiver of the experimental FM based passive radar using software defined radio technology', *International Journal of Electronics and Telecommunications* **58**(4).

Texas Instruments (2011), '10-output low jitter low power differential to lvcmos clock buffer - evaluation board'.

Texas Instruments (2016), 'CDCLVC1310 evaluation module', http://www.ti.com/tool/cdclvc1310-evm. [Online; accessed March-2016].

The Wireless Innovation Forum (2014), 'What is software defined radio', http://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf. [Online; accessed March-2016].

Tigrek, R. F. (2010), A Processing Technique for OFDM-Modulated Wideband Radar Signals, PhD thesis.

Tsao, T., Weiner, D., Varshney, P., Schwarzlander, H., Slamani, M. & Borek, S. (n.d.), Ambiguity function for a bistatic radar, *in* 'Time-Frequency and Time-Scale Analysis, 1992., Proceedings of the IEEE-SP International Symposium', pp. 497–500.

van de Swaluw, M. (2015), 'NT7S's Si5351a VCO hooked up to the local oscillator of a DVB-T dongle.', http://pe1ryy.blogspot.com.au/2015/04/nt7ss-si5351a-vco-hooked-up-to-local.html. [Online; accessed March-2016].

Vandenberg, D. (2012), Mathematical survey and application of the cross-ambiguity function, Master's thesis, Indiana University South Bend, Indiana.

Wang, L. & Yazici, B. (2012), 'Passive imaging of moving targets exploiting multiple scattering using sparse distributed apertures', *IOPscience* **28**(12), 125009.

Whewell, A. (2010), 'Virtual radar server', http://www.virtualradarserver.co.uk. [Online; accessed February-2016].

Whisky, C. (2012), 'Continuous wave radar', http://www.radartutorial.eu/02.basics/Continuous%20Wave%20Radar.en.html. [Online; accessed March-2016].

Wikipedia Contributors (2016), 'List of software-defined radios', https://en.wikipedia.org/w/index.php?title=List_of_software-defined_radios&oldid=719941879. [Online; accessed March-2016].

Willis, N. J. & Griffiths, H. (2007), *Advances in bistatic RADAR*, SciTech Pub., Raleigh, NC.

Wunsch, S. (2016), 'GNU Radio radar toolbox', https://github.com/kit-cel/gr-radar. [Online; accessed March-2016].

YO3IIU (2014), 'RTL2832U based coherent multichannel receiver', http://yo3iiu.ro/blog/. [Online; accessed March-2016].

Appendices

A

Project Specification

University of Southern Queensland

FACULTY OF ENGINEERING AND SURVEYING

ENG4111/ENG4112 Research Project
PROJECT SPECIFICATION

FOR: Mathew Ryan

TITLE: Low cost passive radar through software defined radio

MAJOR: Electrical/Electronic Engineering

SUPERVISORS: Dr Andrew Maxwell
Senior Lecturer (Elec & Comms Engineering), USQ

Mr Liam Price
Director Navy EW and RADAR Engineering, NTB

SPONSORSHIP: Naval Technical Bureau – Department of Defence

ENROLMENT: ENG4111 – EXT, S1 2016
ENG4112 – EXT, S2 2016

PROJECT AIM: To determine the suitability of the Realtek RTL2832u as an interface device for software defined radio passive inverse synthetic aperture radar using DVB-T Broadcasts.

PROGRAMME: (DRAFT, 09 March 2016)

1. Research Passive radar systems and their implementation through software defined radio, the use of DVB-T broadcast signals to produce an ISAR output, and the Realtek RTL2832u TV tuner as a SDR receiver.
2. Develop a test circuit to evaluate the suitability of the RTL28322u receiver.
3. Develop and integrate software to interface the receiver and produce a radar display.
4. Test the circuit and software in a simulated and real world environment.
5. Evaluate the results achieved in the testing.
6. Evaluate the suitability of the Realtek R2832u as the hardware receiver in a passive inverse synthetic aperture radar.

If time and resources permit:

7. Identify and implement improvements in the circuitry to increase the reliability of the radar display..

B

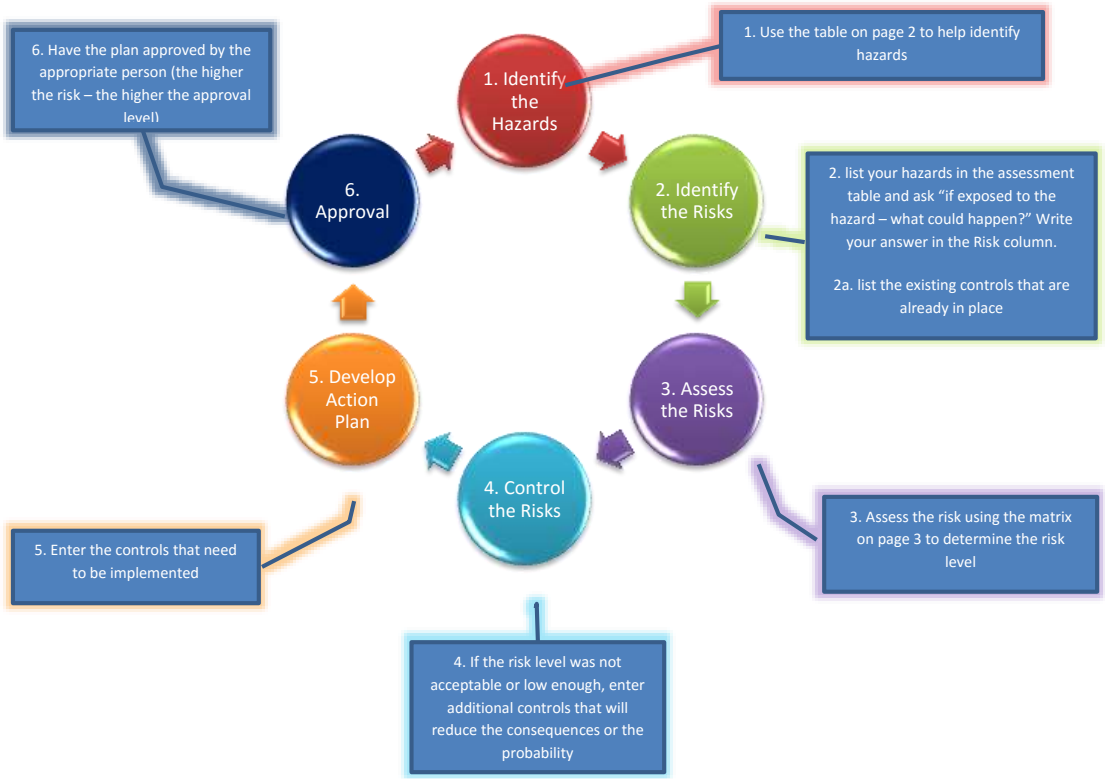
Risk Assessment

University of Southern Queensland

Risk Management Plan

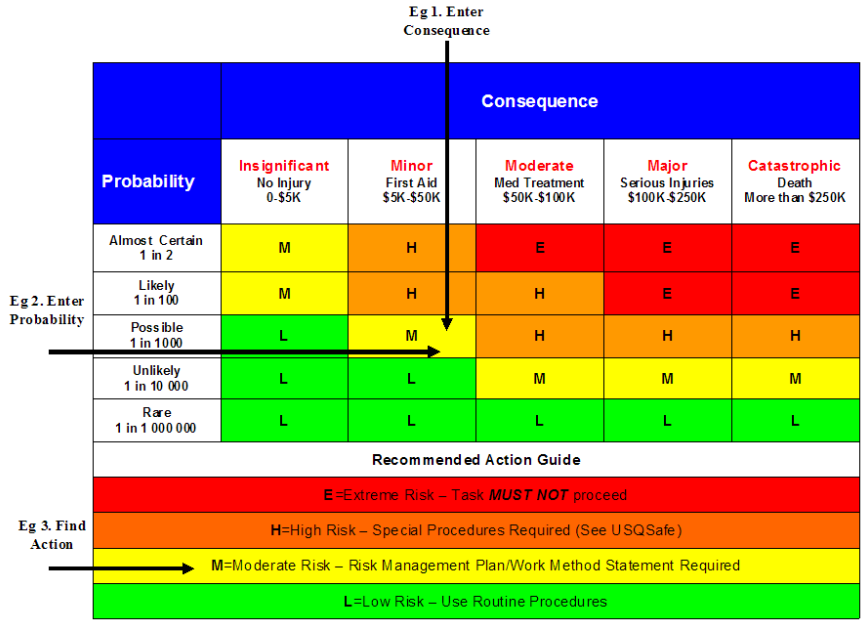
Workplace (Division/Faculty/Section): Faculty of Health, Engineering & Sciences		
Assessment No (if applicable): ERP2016 – ENG4111 & ENG4112	Assessment Date: 25/04/2016	Review Date: 01/10/2016
Context: What is being assessed? Describe the item, job, process, work arrangement, event etc: Low Cost Passive Radar Through Software Defined Radio		
Assessment Team – who is conducting the assessment?		
Assessor(s): Mathew Ryan Others consulted: Liam Price (Director of Navy EW and RADAR Engineering), Robert Koerner (Senior Weapons Systems & Electrical Maintenance Officer), Michael Gall (Mechanical Technician)		

The Risk Management Process



Step 1 - **Identify the hazards** (use this table to help identify hazards then list all hazards in the risk table)		
General Work Environment		
☒ Sun exposure	☐ Water (creek, river, beach, dam)	☐ Sound / Noise
☐ Animals / Insects	☒ Storms / Weather/Wind/Lightning	☒ Temperature (heat, cold)
☒ Air Quality	☒ Lighting	☐ Uneven Walking Surface
☒ Trip Hazards	☐ Confined Spaces	☐ Restricted access/egress
☐ Pressure (Diving/Altitude)	☒ Smoke	☐
Other/Details:		
Machinery, Plant and Equipment		
☐ Machinery (fixed plant)	☐ Machinery (portable)	☒ Hand tools
☐ Laser (Class 2 or above)	☐ Elevated work platforms	☐ Traffic Control
☐ Non-powered equipment	☐ Pressure Vessel	☒ Electrical
☐ Vibration	☐ Moving Parts	☐ Acoustic/Noise
☒ Vehicles	☐ Trailers	☒ Hand tools
Other/Details:		
Manual Tasks / Ergonomics		
☒ Manual tasks (repetitive, heavy)	☒ Working at heights	☐ Restricted space
☐ Vibration	☐ Lifting Carrying	☐ Pushing/pulling
☐ Reaching/Overstretching	☒ Repetitive Movement	☒ Bending
☒ Eye strain	☐ Machinery (portable)	☒ Hand tools
Other/Details:		
Biological (e.g. hygiene, disease, infection)		
☐ Human tissue/fluids	☐ Virus / Disease	☐ Food handling
☐ Microbiological	☐ Animal tissue/fluids	☐ Allergenic
Other/Details:		
Chemicals Note: Refer to the label and Safety Data Sheet (SDS) for the classification and management of all chemicals.		
☐ Non-hazardous chemical(s)	☐ 'Hazardous' chemical (Refer to a completed hazardous chemical risk assessment)	
☐ Engineered nanoparticles	☐ Explosives	☐ Gas Cylinders
Name of chemical(s) / Details:		
Critical Incident – resulting in:		
☐ Lockdown	☐ Evacuation	☐ Disruption
☐ Public Image/Adverse Media Issue	☐ Violence	☐ Environmental Issue
Other/Details:		
Radiation		
☐ Ionising radiation	☐ Ultraviolet (UV) radiation	☒ Radio frequency/microwave
☐ infrared (IR) radiation	☐ Laser (class 2 or above)	☐
Other/Details:		
Energy Systems – incident / issues involving:		
☐ Electricity (incl. Mains and Solar)	☐ LPG Gas	☐ Gas / Pressurised containers
Other/Details:		
Facilities / Built Environment		
☒ Buildings and fixtures	☐ Driveway / Paths	☒ Workshops / Work rooms
☐ Playground equipment	☐ Furniture	☐ Swimming pool
Other/Details:		
People issues		
☒ Students	☒ Staff	☒ Visitors / Others
☐ Physical	☐ Psychological / Stress	☐ Contractors
☐ Fatigue	☐ Workload	☐ Organisational Change
☐ Workplace Violence/Bullying	☐ Inexperienced/new personnel	☐
Other/Details:		

Risk Matrix



Probability	Consequence				
	Insignificant No Injury 0-$5K	Minor First Aid $5K-$50K	Moderate Med Treatment $50K-$100K	Major Serious Injuries $100K-$250K	Catastrophic Death More than $250K
Almost Certain 1 in 2	M	H	E	E	E
Likely 1 in 100	M	H	H	E	E
Possible 1 in 1000	L	M	H	H	H
Unlikely 1 in 10 000	L	L	M	M	M
Rare 1 in 1 000 000	L	L	L	L	L

Recommended Action Guide

E=Extreme Risk – Task ***MUST NOT*** proceed

H=High Risk – Special Procedures Required (See USQSafe)

M=Moderate Risk – Risk Management Plan/Work Method Statement Required

L=Low Risk – Use Routine Procedures

Risk register and Analysis

Step 1 (cont)	Step 2	Step 2a	Step 3			Step 4				
Hazards: From step 1 or more if identified	**The Risk:** What can happen if exposed to the hazard with existing controls in place?	**Existing Controls:** What are the existing controls that are already in place?	**Risk Assessment:** (use the Risk Matrix on p3) Consequence x Probability = Risk Level			**Additional controls:** Enter additional controls if required to reduce the risk level	**Risk assessment with additional controls:** (use the Risk Matrix on p3 – has the consequence or probability changed?)			**Controls Implemented? Yes/No**
			Consequence	**Probability**	**Risk Level**		**Consequence**	**Probability**	**Risk Level**	
Sun exposure during experiment	Sun exposure leading to heat stress/heat stroke/exhaustion and sun burn leading to serious personal injury	Regular breaks, chilled water, sun screen and appropriate clothing.	Catastrophic	Possible	High	Limit exposure time, buddy system and temporary shade	Catastrophic	Unlikely	Moderate	Yes
Air quality during soldering	Exposure to fumes leading to respiratory problems	Ventilation is appropriate, limit exposure proximity to work area.	Major	Likely	Extreme	Soldering to be conducted in a well-ventilated area. Appropriate respiratory PPE to be worn.	Major	Possible	High	Yes
Smoke and fumes from soldering	Exposure to smoke and fumes leading to respiratory problems	Ventilation is appropriate, limit exposure proximity to work area.	Major	Likely	Extreme	work to be conducted in a well-ventilated area. Appropriate respiratory PPE to be worn.	Major	Possible	High	Yes
Lighting	Low or extreme light exposure leading to strain on eyes	Ensure that lighting is appropriate for the activity. Use desk lamps to ensure activities are appropriately lit.	Minor	Possible	Moderate	Ensure that lighting is appropriate for the activity. Use desk lamps to ensure activities are appropriately lit.	Minor	Unlikely	Low	Yes
Working with Radio Frequency	Extended exposure to unsafe levels of Electromagnetic waves leading to health issues with body tissue.	Minimise exposure time to Electromagnetic waves and avoid direct contact with the transmitter.	Moderate	Possible	High	Minimise exposure time to Electromagnetic waves and avoid direct contact with transmitter.	Moderate	Possible	High	Yes
Working with tools at high temperature	High temperature exposure leading to serious burns	Tools are handled and stored in the correct manner. Allow sufficient cooling time.	Major	Possible	High	Components are held in place using mechanical means while using high temperature tools.	Major	Unlikely	Moderate	Yes
Working with materials at high temperature	High temperature exposure leading to serious burns	No direct contact with high temperature materials. Allow sufficient cooling time.	Major	Possible	High	Appropriate material handling techniques are in place to avoid contact with high temperature i.e. use of pliers and tweezers to handle hot components.	Major	Unlikely	Moderate	Yes
Vehicles	Use of a vehicle leading to car accident causing serious personal injury/death	Drive according to the road conditions and IAW road rules.	Catastrophic	Possible	High	Drive according to the road conditions and IAW road rules.	Catastrophic	Possible	High	Yes
High voltage electrical exposure	Electric shock leading to serious personal injury/death	Ensure high voltage devices are suitably isolated before any contact is made.	Catastrophic	Possible	High	Ensure that devices are disconnected from power before they are touched.	Catastrophic	Unlikely	Moderate	Yes
Manual handling of heavy objects	Manual handling of heavy plates leading to serious back injury	Ensure that a maximum of one plate is carried at a time. Maximum weight allowed to be carried by one person is 10kg.	Major	Unlikely	High	Ensure that a maximum of one plate is carried at a time. Maximum weight allowed to be carried by one person is 10kg.	Major	Unlikely	Moderate	Yes
Bending while carrying objects	Bending during manual handling leading to serious personal injury	Back is kept straight and knees bent while carrying any object.	Major	Almost Certain	Extreme	Ensure a buddy system or mechanical means in place while carrying any object over 10kg.	Major	Unlikely	Moderate	Yes
Trip Hazard over Cables	Tripping over cables in situ for conducting the experiment	Ensure all cables are suitably restrained and away from walkways or working areas	Moderate	Unlikely	Moderate	Cable tie and bind all cables to ensure they are away from walkways and work areas	Moderate	Rare	Low	Yes

Step 1 (cont)	Step 2	Step 2a	Step 3			Step 4				
Hazards: From step 1 or more if identified	**The Risk:** What can happen if exposed to the hazard with existing controls in place?	**Existing Controls:** What are the existing controls that are already in place?	**Risk Assessment:** (use the Risk Matrix on p3) Consequence x Probability = Risk Level			**Additional controls:** Enter additional controls if required to reduce the risk level	**Risk assessment with additional controls:** (use the Risk Matrix on p3 – has the consequence or probability changed?)			**Controls Implemented? Yes/No**
			Consequence	**Probability**	**Risk Level**		**Consequence**	**Probability**	**Risk Level**	
Storms & Lightning risk to receiver antenna in high positions	Receive antennas must be located up high, increasing the risk that they will act as a lightning rod and attract electrical energy	Testing should not be undertaken during storm conditions.	Catastrophic	Unlikely	Moderate	Additional earthing can be added to the antenna and coaxial cable with an earth stake to reduce the damage.	Catastrophic	Unlikely	Moderate	Yes
Repetitive manual tasks	The typing required to produce the dissertation and program the radar receiver can cause injury	Taking regular breaks and following good WHS practice for repetitive tasks	Moderate	Possible	High	Taking regular breaks and following good WHS practice for repetitive tasks	Moderate	Unlikely	Moderate	Yes
Working at Heights	Receive antennas must be placed in high locations, falling whilst working on the antenna can cause injury	Use of a buddy system when aloft	Catastrophic	Possible	High	Use of a buddy system when aloft and undertake working at heights training to ensure awareness	Catastrophic	Unlikely	Moderate	Yes

Step 5 – Action Plan (for controls not already in place)

Control Option	Resources	Person(s) responsible	Proposed implementation date

Step 6 – Approval

Drafter's Comments:

All additional controls have been implemented.

Drafter Details:

Name: Mathew Ryan Signature: Date: 25/04/2016

Assessment Approval: (Extreme or High = VC, Moderate = Cat 4 delegate or above, Low = Manager/Supervisor)

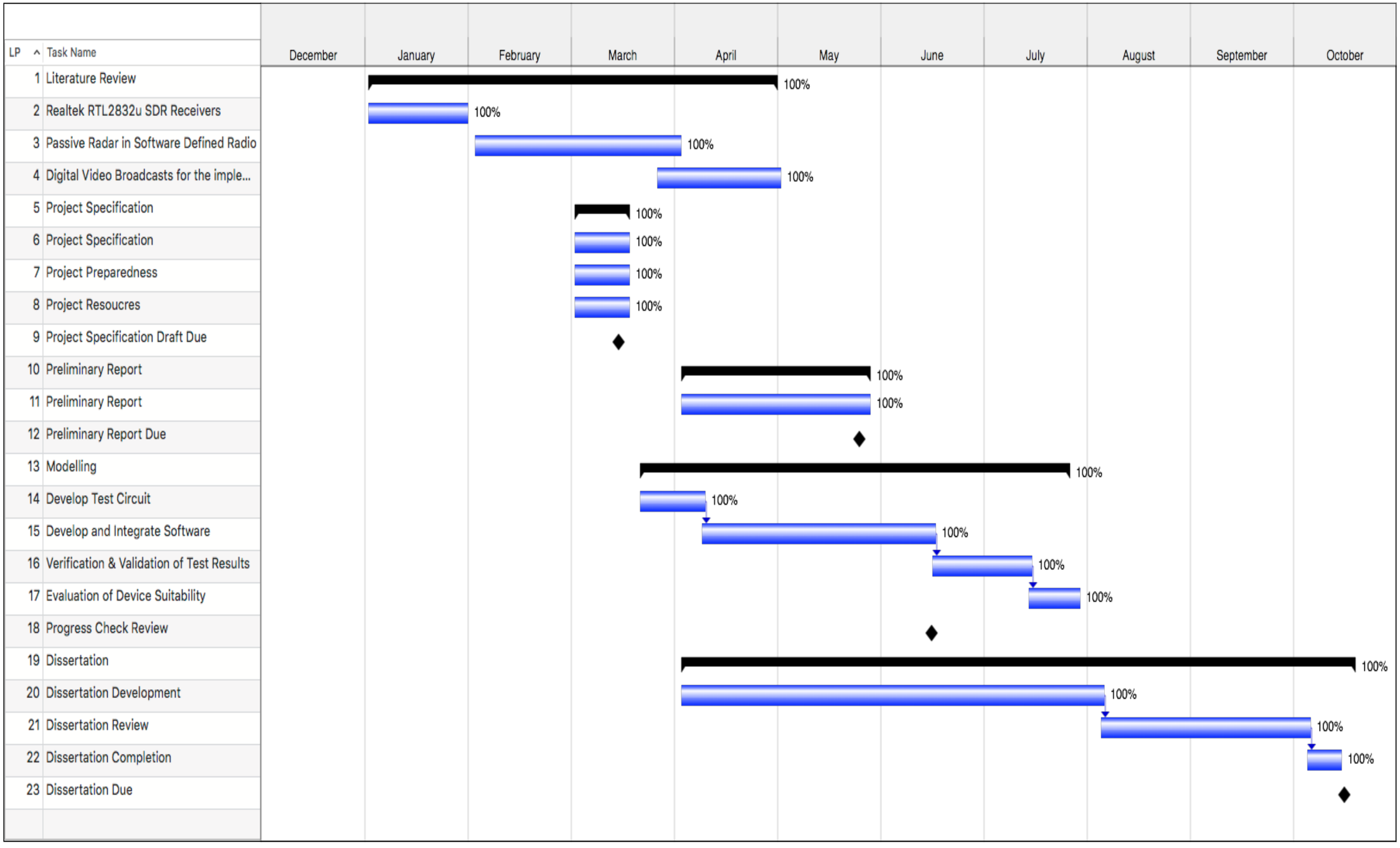
I am satisfied that the risks are as low as reasonably practicable and that the resources required will be provided.

Name: Signature: Date: / /

Position Title:

C

Project Timeline


LP
Task Name
December
January
February
March
April
May
June
July
August
September
October
1 Literature Review
2 Realtek RTL2832u SDR Receivers
3 Passive Radar in Software Defined Radio
4 Digital Video Broadcasts for the imple...
5 Project Specification
6 Project Specification
7 Project Preparedness
8 Project Resoucres
9 Project Specification Draft Due
10 Preliminary Report
11 Preliminary Report
12 Preliminary Report Due
13 Modelling
14 Develop Test Circuit
15 Develop and Integrate Software
16 Verification & Validation of Test Results
17 Evaluation of Device Suitability
18 Progress Check Review
19 Dissertation
20 Dissertation Development
21 Dissertation Review
22 Dissertation Completion
23 Dissertation Due
100%

D

Project Resources

A listing of all relevant project resources is included within the tables below. Resources that are used indirectly or were not specifically procured for the undertaking of the project, have not been included within the tables.

Product	Product Number	Supplier	Qty	Cost
RTL2832U Based USB TV Receiver	N/A	eBay	4	13.60
SMA (M) to MMCX (F) Adapter	N/A	eBay	3	2.19
BNC (F) to SMA (M) Adapter	N/A	eBay	3	1.87
SMA (F) to BNC (M) Adapter	N/A	eBay	3	1.52
SMA (M) to SMA (M) Patch Cable (30cm)	N/A	eBay	3	2.08
BNC Bulkhead (F) to SMA (M) Patch Cable (50cm)	N/A	eBay	3	3.98
Right Angle SMA (F) PCB Solder Mount	5-1814400-1	Element14	10	2.37
Verbatim 16GB USB Flash Drive 3 Pack	759481	JB Hi-Fi	1	29.95
0805 82 Ohm SMD Resistor 0.125W 25ppm	565863	RS Component	10	4.70
SMA (F) Edge Launch Connector	AF-1865	Little Bird Electronics	6	3.77
Adafruit Si5351A Clock Generator Board	AF-2045	Little Bird Electronics	1	12.01
10nF Ceramic Capacitor 50V	RC5348	Jaycar	4	0.16
3mm Desolder Braid	NS3028	Jaycar	1	5.95
Metal Bench Enclosure	HB5556	Jaycar	1	53.95
10 Port USB 2.0 Hub	XC4946	Jaycar	1	53.95
Arduino LeoStick Development Board	XC4266	Jaycar	1	43.15
Arduino LeoStick Prototype Sheild	XC4268	Jaycar	1	8.75
Jumper Lead Plug to Plug	WC6025	Jaycar	1	5.35
Jumper Lead Plug to Socket	WC6028	Jaycar	1	5.35
USB 2.0 A-B Cable (0.5m)	WC7705	Jaycar	1	5.25
1.5mm Desolder Braid	NS3026	Jaycar	1	5.25
Hookup Wire, Black (25m)	WH3001	Jaycar	1	4.90
Metal PCB Spacer (M3 x 10mm)	HP0900	Jaycar	1	3.45
28 Way Vertical Single Header	HM3211	Jaycar	1	0.75

Table D.1: Low Cost Passive SDR Hardware Resource Costing.

Product	Product Number	Supplier	Qty	Cost
433Mhz Antenna SMA (M) Right Angle	N/A	eBay	5	1.76
433 Mhz ASK Receiver Module	ZW3102	Jaycar	1	13.95
Basic Proto Sheild for Arduino	XC4214	Jaycar	2	4.45
Arduino Stackable Header Set	HM3207	Jaycar	2	3.75
BNC (M) to BNC (M) Patch Lead (1.5m)	WV7300	Jaycar	1	9.95
BNC (M) to F-Type (F) Adapter	PP0650	Jaycar	1	3.25
Arduino Uno Development Board	XC4410	Jaycar	1	26.95
Arduino RF Transceiver Module	XC4522	Jaycar	1	17.95
433 Mhz ASK Transmitter Module	ZW3100	Jaycar	1	12.35
UHF Log Periodic Yagi Antenna	N/A	eBay	2	30.00

Table D.2: SDR Verification Testing Resource Costing.

Product	Product Number	Supplier	Qty	Cost
Wireless Keyboard and Mouse	N/A	Apple	1	130.00
Mini Display Port to DVI Adapter	WQ7444	Jaycar	1	29.95
iPhone Field Strength Meter Adapter	QM1678	Jaycar	1	34.95

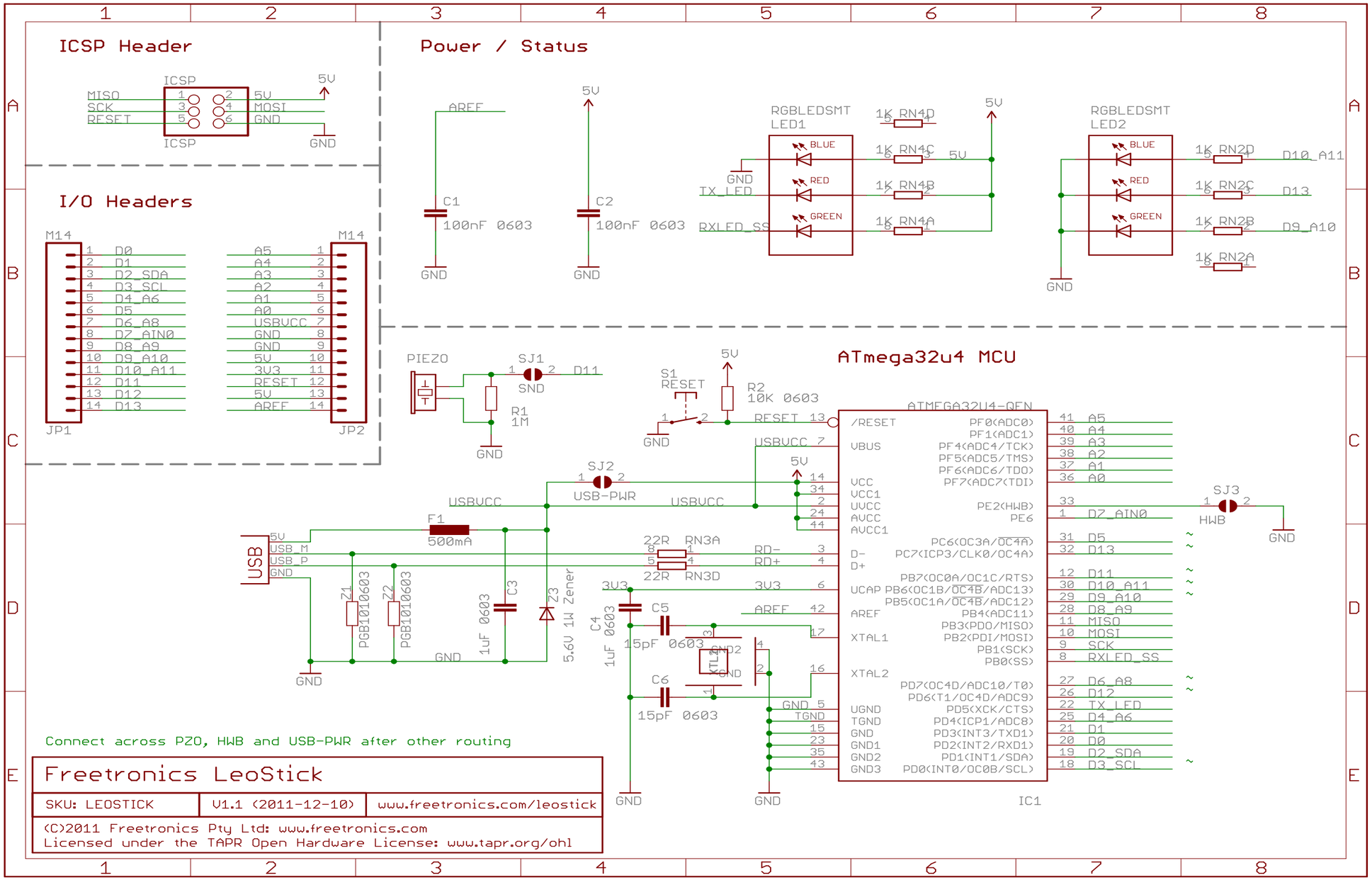
Table D.3: WHS Resource Costing.

Product	Product Number	Supplier
Oscilloscipe	TDS3054C	Tektronix

Table D.4: Calibrated Test Equipment.

E

Freetronics Arduino Compatible Leostick Device Schematic


ICSP Header
ICSP
MISO
SCK
RESET
5V
MOSI
GND
I/O Headers
M14
JP1
JP2
D0
D1
D2_SDA
D3_SCL
D4_A6
D5
D6_A8
D7_AIN0
D8_A9
D9_A10
D10_A11
D11
D12
D13
A5
A4
A3
A2
A1
A0
USBVCC
3V3
RESET
AREF
Power / Status
AREF
C1
100nF 0603
C2
RGBLEDSMT
LED1
LED2
BLUE
RED
GREEN
1K RN4D
1K RN4C
1K RN4B
1K RN4A
1K RN2D
1K RN2C
1K RN2B
1K RN2A
TX_LED
RXLED_SS
PIEZO
SJ1
SND
R1
1M
ATmega32u4 MCU
S1
RESET
R2
10K 0603
ATMEGA32U4-QFN
/RESET
VBUS
VCC
VCC1
UVCC
AVCC
AVCC1
D-
D+
UCAP
AREF
XTAL1
XTAL2
UGND
TGND
GND
GND1
GND2
GND3
PF0(ADC0)
PF1(ADC1)
PF4(ADC4/TCK)
PF5(ADC5/TMS)
PF6(ADC6/TDO)
PF7(ADC7/TDI)
PE2(HWB)
PE6
PC6(OC3A/OC4A)
PC7(ICP3/CLK0/OC4A)
PB7(OC0A/OC1C/RTS)
PB6(OC1B/OC4B/ADC13)
PB5(OC1A/OC4B/ADC12)
PB4(ADC11)
PB3(PDO/MISO)
PB2(PDI/MOSI)
PB1(SCK)
PB0(SS)
PD7(OC4D/ADC10/T0)
PD6(T1/OC4D/ADC9)
PD5(XCK/CTS)
PD4(ICP1/ADC8)
PD3(INT3/TXD1)
PD2(INT2/RXD1)
PD1(INT1/SDA)
PD0(INT0/OC0B/SCL)
IC1
SJ2
USB-PWR
SJ3
HWB
USB
F1
500mA
22R RN3A
22R RN3D
RD-
RD+
Z1
Z2
PGB1010603
C3
1uF 0603
Z3
5.6V 1W Zener
C4
1uF 0603
C5
15pF 0603
C6
15pF 0603
XTAL1
GND2
Connect across PZO, HWB and USB-PWR after other routing
Freetronics LeoStick
SKU: LEOSTICK
V1.1 (2011-12-10)
www.freetronics.com/leostick
(C)2011 Freetronics Pty Ltd: www.freetronics.com
Licensed under the TAPR Open Hardware License: www.tapr.org/ohl

F

Timing Source Generator Source Code

The program `RadarClockGen.ino` uses the Adafruit library to produce a 28.8 MHz clock frequency output on 3 separate channels.

Listing F.1: RadarClockGen.ino

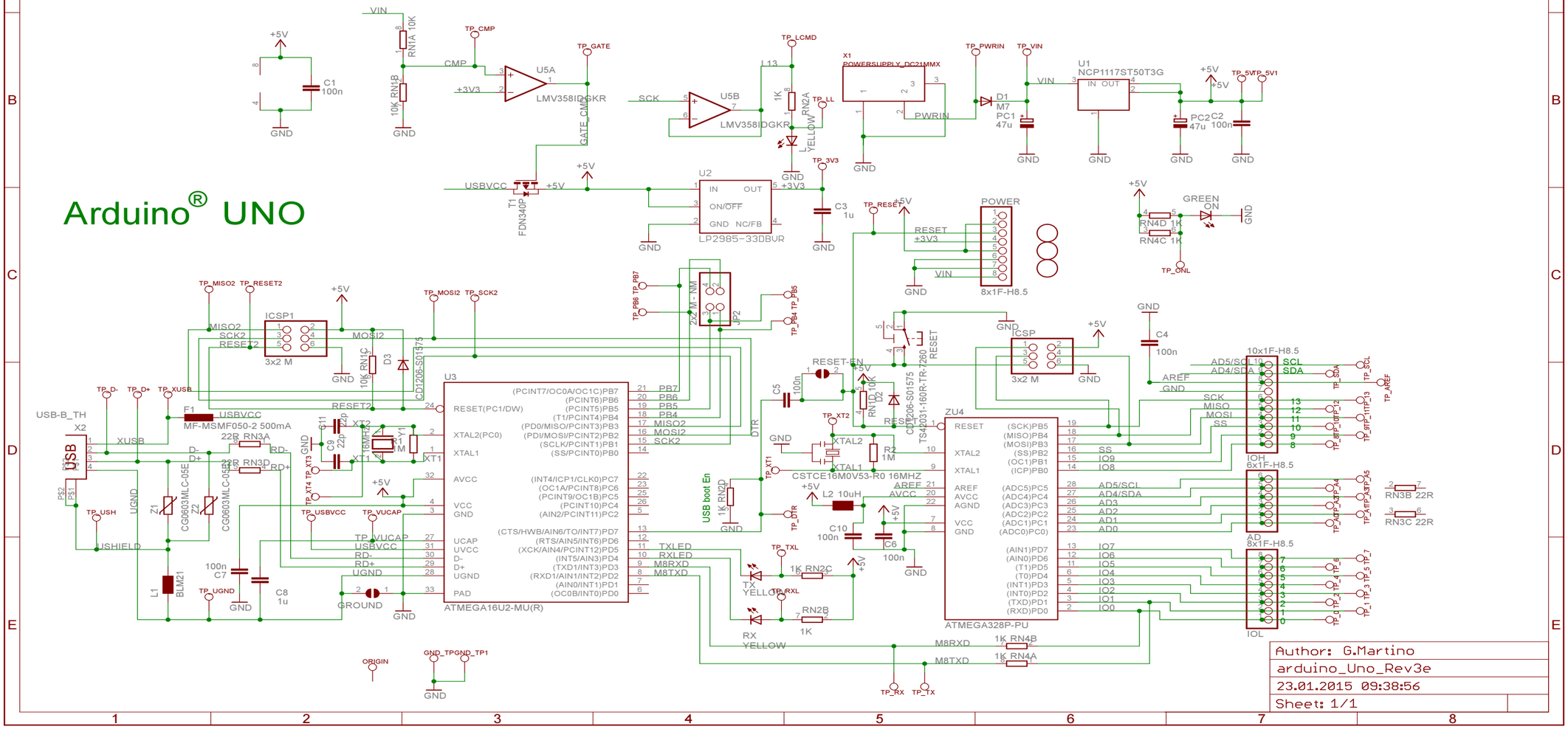
```
/*
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% ERP2016: Engineering Research Project 2016            %
% Passive Radar Processing                              %
% External Clock Generator                              %
% Compiled 20 July 2016                                 %
% Student Name: Mathew Ryan                             %
% Student ID: 0061010502                                %
% File Title: Radar_Clock_Gen                           %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


%% PROGRAM DESCRIPTION
%  Generates clock signal at 28.8 MHz and flashes LED
*/

// Include Libraries
#include <Wire.h>
#include <Adafruit_SI5351.h>

// Set Clock Generator Label
Adafruit_SI5351 clockgen = Adafruit_SI5351();

void setup(void)
{
  // Define Serial Baudrate
  Serial.begin(9600);
  // Print Serial Data
  Serial.println("Si5351 Clockgen Test"); Serial.println("");

  // Initialise the sensor
  if (clockgen.begin() != ERROR_NONE)
  {
    //There was a problem detecting the IC ... check your connections
    Serial.print("Ooops, no Si5351 detected ... Check your wiring or I2C ADDR!");
    while(1);
  }
  Serial.println("OK!");

  // Serial Print Status
  Serial.println("Set PLLA to 640MHz");
  // Set PLL A Frequency
  clockgen.setupPLL(SI5351_PLL_A, 25, 3, 5);
  // Serial Print Status
  Serial.println("Set PLLB to 806.4MHz");
```

```
  // Set PLL B Frequency
  clockgen.setupPLL(SI5351_PLL_B, 32, 32, 125);

  // Optional 160 MHz Reference Frequency
  // Serial.println("Set Output #0 to 160.00MHz");
  // clockgen.setupMultisynth(0, SI5351_PLL_A, 4, 0, 1);

  // Set Output 0 to 28.8 MHz
  Serial.println("Set Output #0 to 28.80MHz");
  clockgen.setupMultisynth(0, SI5351_PLL_B, 28, 0, 1);

  // Set Output 1 to 28.8 MHz
  Serial.println("Set Output #1 to 28.80MHz");
  clockgen.setupMultisynth(1, SI5351_PLL_B, 28, 0, 1);

  // Set Output 2 to 28.8 MHz
  Serial.println("Set Output #2 to 28.80MHz");
  clockgen.setupMultisynth(2, SI5351_PLL_B, 28, 0, 1);

  // Enable the clocks
  clockgen.enableOutputs(true);

  // initialize digital pins as an output.
  pinMode(9, OUTPUT);
  pinMode(10, OUTPUT);
  pinMode(13, OUTPUT);

}

void loop() {
  digitalWrite(9, HIGH);    // turn the LED on (HIGH is the voltage level)
  delay(1000);              // wait for a second
  digitalWrite(9, LOW);     // turn the LED off by making the voltage LOW
  digitalWrite(10, HIGH);   // turn the LED on (HIGH is the voltage level)
  delay(1000);              // wait for a second
  digitalWrite(10, LOW);    // turn the LED off by making the voltage LOW
  digitalWrite(13, HIGH);   // turn the LED on (HIGH is the voltage level)
  delay(1000);              // wait for a second
  digitalWrite(13, LOW);    // turn the LED off by making the voltage LOW
}
```

G

Arduino Uno Device Schematic

Arduino® UNO



H

Continuous Wave Transmitter Source Code

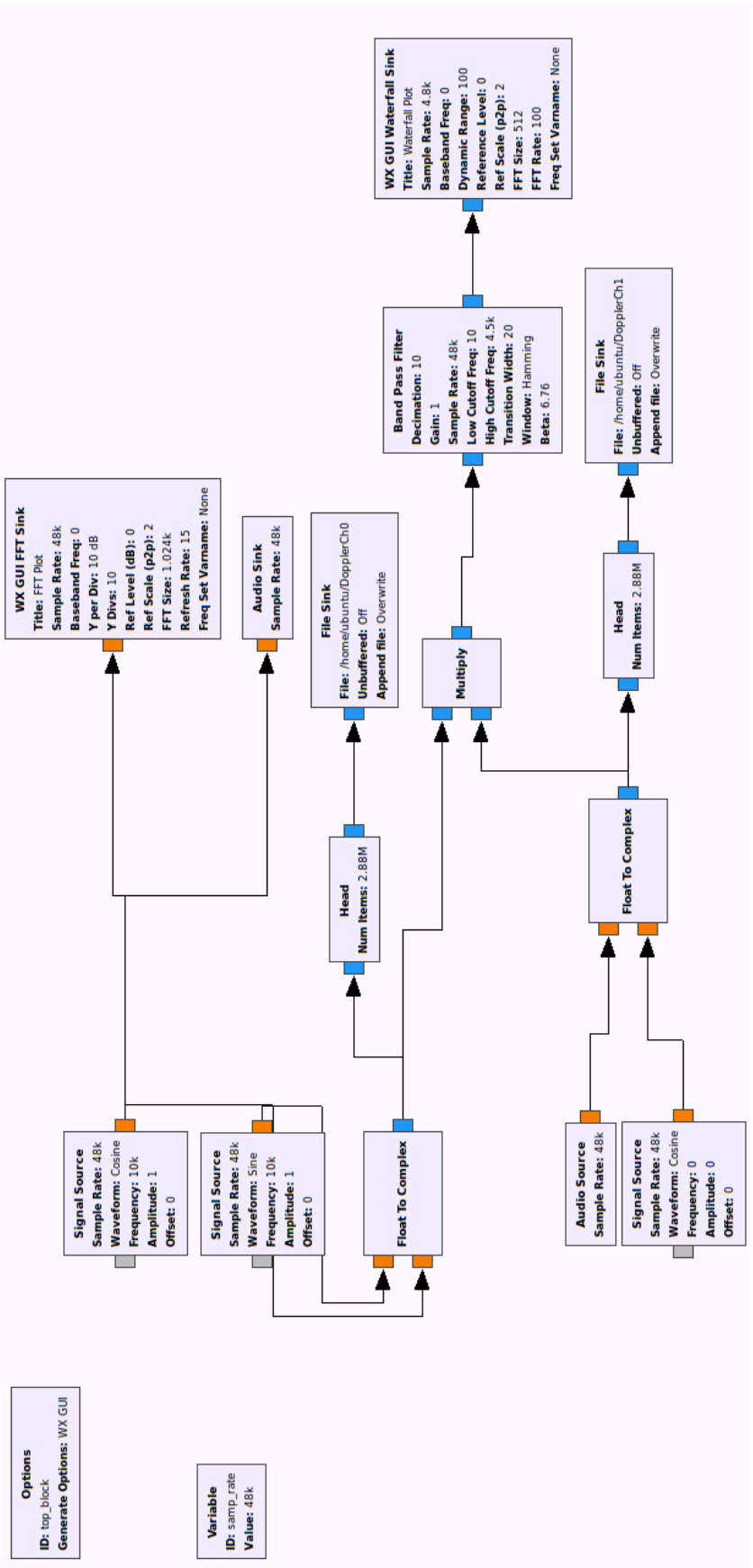
The program `TXOutputSet.ino` switches the OOK data input of the 433 MHz transmitter high to provide a continuous wave signal.

Listing H.1: TXOutputSet.ino

```
/*
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% ERP2016: Engineering Research Project 2016                            %
% Passive Radar Processing                                              %
% External Clock Generator                                              %
% Compiled 20 July 2016                                                 %
% Student Name: Mathew Ryan                                             %
% Student ID: 0061010502                                                %
% File Title: TX_Output_Set                                             %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


%% PROGRAM DESCRIPTION
%  Sets 433 MHz continuous wave output
*/


// the setup function runs once when you press reset or power the board
void setup() {
  // initialize digital pin 3 as an output.
  pinMode(3, OUTPUT);
}

// the loop function runs over and over again forever
void loop() {
  digitalWrite(3, HIGH);    // turn the LED on (HIGH is the voltage level)
  delay(1000);              // wait for a second
}
```

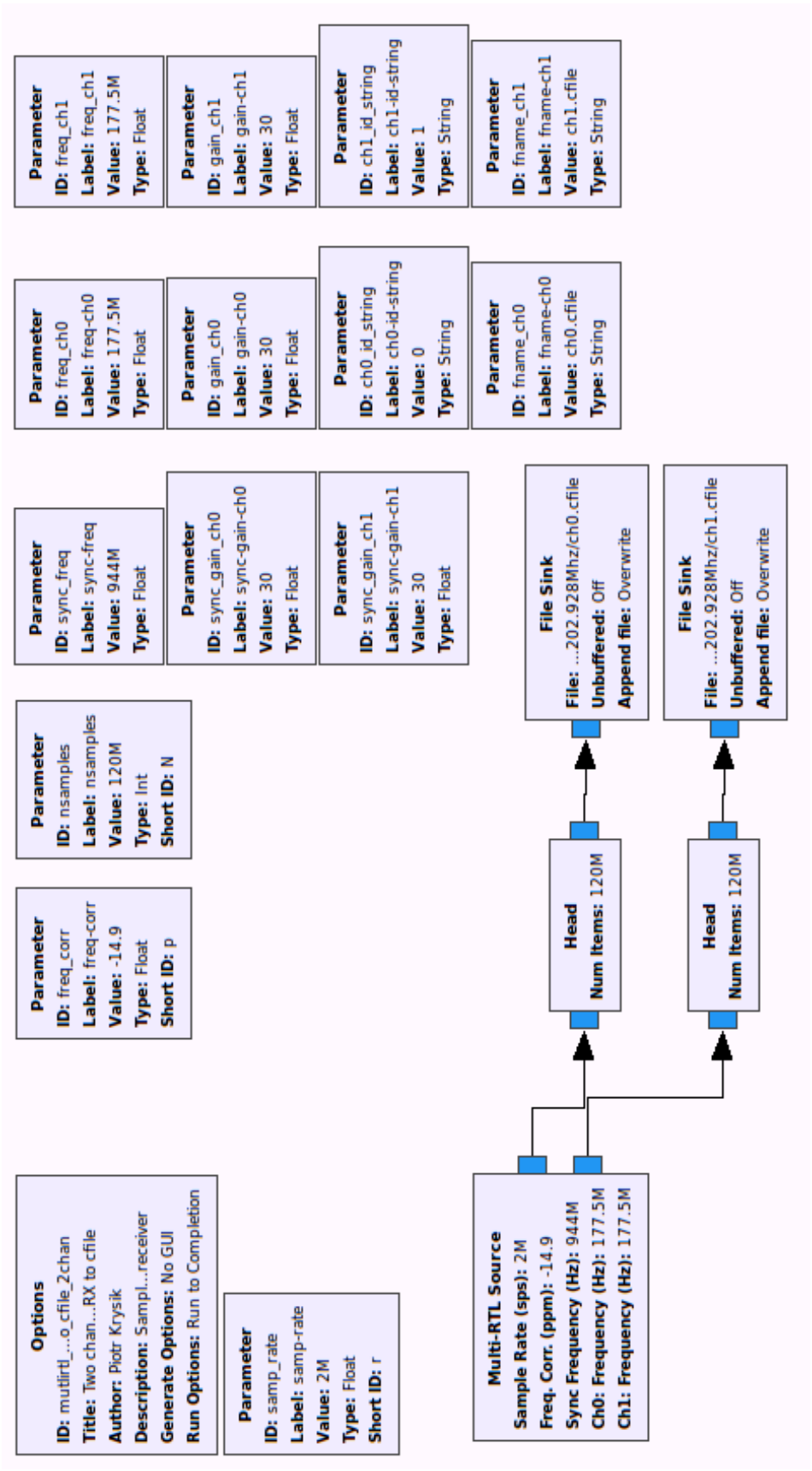
I

Doppler Radar Software Verification Flowgraph


WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 4.8k
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 100
Freq Set Varname: None
Band Pass Filter
Decimation: 10
Gain: 1
Sample Rate: 48k
Low Cutoff Freq: 10
High Cutoff Freq: 4.5k
Transition Width: 20
Window: Hamming
Beta: 6.76
File Sink
File: /home/ubuntu/DopplerCh1
Unbuffered: Off
Append file: Overwrite
WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 48k
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None
Audio Sink
Sample Rate: 48k
File Sink
File: /home/ubuntu/DopplerCh0
Unbuffered: Off
Append file: Overwrite
Multiply
Head
Num Items: 2.88M
Head
Num Items: 2.88M
Float To Complex
Signal Source
Sample Rate: 48k
Waveform: Cosine
Frequency: 10k
Amplitude: 1
Offset: 0
Signal Source
Sample Rate: 48k
Waveform: Sine
Frequency: 10k
Amplitude: 1
Offset: 0
Float To Complex
Audio Source
Sample Rate: 48k
Signal Source
Sample Rate: 48k
Waveform: Cosine
Frequency: 0
Amplitude: 0
Offset: 0
Options
ID: top_block
Generate Options: WX GUI
Variable
ID: samp_rate
Value: 48k

J

Multi-RTL Coherent Data Acquisition Flowgraph


Options
ID: mutlirtl_...o_cfile_2chan
Title: Two chan...RX to cfile
Author: Piotr Krysik
Description: Sampl...receiver
Generate Options: No GUI
Run Options: Run to Completion
Parameter
ID: samp_rate
Label: samp-rate
Value: 2M
Type: Float
Short ID: r
Parameter
ID: freq_corr
Label: freq-corr
Value: -14.9
Type: Float
Short ID: p
Parameter
ID: nsamples
Label: nsamples
Value: 120M
Type: Int
Short ID: N
Parameter
ID: sync_freq
Label: sync-freq
Value: 944M
Type: Float
Parameter
ID: sync_gain_ch0
Label: sync-gain-ch0
Value: 30
Type: Float
Parameter
ID: sync_gain_ch1
Label: sync-gain-ch1
Value: 30
Type: Float
Parameter
ID: freq_ch0
Label: freq-ch0
Value: 177.5M
Type: Float
Parameter
ID: gain_ch0
Label: gain-ch0
Value: 30
Type: Float
Parameter
ID: ch0_id_string
Label: ch0-id-string
Value: 0
Type: String
Parameter
ID: fname_ch0
Label: fname-ch0
Value: ch0.cfile
Type: String
Parameter
ID: freq_ch1
Label: freq_ch1
Value: 177.5M
Type: Float
Parameter
ID: gain_ch1
Label: gain-ch1
Value: 30
Type: Float
Parameter
ID: ch1_id_string
Label: ch1-id-string
Value: 1
Type: String
Parameter
ID: fname_ch1
Label: fname-ch1
Value: ch1.cfile
Type: String
Multi-RTL Source
Sample Rate (sps): 2M
Freq. Corr. (ppm): -14.9
Sync Frequency (Hz): 944M
Ch0: Frequency (Hz): 177.5M
Ch1: Frequency (Hz): 177.5M
Head
Num Items: 120M
Head
Num Items: 120M
File Sink
File: ...202.928Mhz/ch0.cfile
Unbuffered: Off
Append file: Overwrite
File Sink
File: ...202.928Mhz/ch1.cfile
Unbuffered: Off
Append file: Overwrite

K

Complex Ambiguity Function Peak Value Calculation MATLAB Function

The function `CAF.m` calculates the peak values of the complex ambiguity function for time deviation (TDOA) and frequency deviation (FDOA). The function was developed by Johnson (2001).

Listing K.1: Complex Ambiguity Function Calculation Developed By LCDR J.J.Johnson

```
function [TDOA, FDOA] = CAF(S1, S2, Max_f, fs, Max_t)

% ********************************************************************
% CAF takes as inputs two sampled signal vectors (S1 & S2) in analytic
% signal format, the maximum expected FDOA in Hertz (Max_f), the
% sampling frequency used to generate S1 & S2 (fs), and the maximum
% expected TDOA in seconds (Max_t). The function then utilizes
% Stein's method in [1] to compute coarse estimations of TDOA and
% FDOA between S1 & S2. Finally, "fine mode" calcualtions are made
% to compute the final TDOA and FDOA, which are returned to the
% user via the output arguments.

% Written by: LCDR Joe J. Johnson, USN
% Last modified: 17 September 2001
% ********************************************************************

%clc;

N = length(S1);
S1 = reshape(S1,N,1);           % Ensures signals are column vectors due to
S2 = reshape(S2,N,1);           % Matlab's better efficiency on columns

S1_orig = S1;                   % Want to preserve original input signals
S2_orig = S2;                   % for later use; S1 & S2 will be
                                % manipulated in the fine mode below.

% The following while loop ensures that the sub-block size, N1, is
% large enough to ensure proper resolution. If Max_f/fs*N1 were
% less than 1, then the Freq calculated at the end would always be
% + or - 1/N1! 2^19 = 524288 is about the limit for efficient
% processing speed.
N1=1024;
while (Max_f/fs*N1 < 2) && (N1 < 2^19)
    N1 = 2*N1;
end

N2=N1/2;

if N1 > N                       % For cases where resolution calls for
    S1 = [S1;zeros(N1-N,1)];    % a sub-block size larger than the
    S2 = [S2;zeros(N1-N,1)];    % signal vectors, pad the vectors with
    N = N1;                     % zeros so that they have a total of
end                             % N1 elements.
```

```
% Want magnitude of Max_f, since +&- will be used below
Max_f = abs(Max_f);
Number_of_Blocks = length(S1)/N1;       % Number of sub-blocks to break
                                        % the signal into

Min_v = floor(-Max_f/fs*N1);            % Smallest freq bin to search
Max_v = -Min_v;                         % Largest freq bin to search
v_values = Min_v : Max_v;               % Vector of all bins to search

Max_samples = Max_t * fs;           % Maximum number of samples to search

% Finds max number of block shifts (q) that must occur for each
% R and v below.
if Max_samples > N2
    q_max = min(ceil((Max_samples - N2)/N1),Number_of_Blocks-1);
else q_max = 0;
end

x=0;
divisors = Number_of_Blocks:-1:1;       % Used to scale "temp" below...


% ********************************************************************
% COARSE MODE computations.
% ********************************************************************

for v = 1:length(v_values)
    temp(1:N1,1:floor(q_max)+1)=0; % Initializing -- saves time....
    for R = 0:Number_of_Blocks-1

        % temp1 is the FFT of the R'th block of S1, shifted by "v" bins.
        temp1 = fftshift(fft(S1(1+R*N1 : N1*(R+1))));
        temp1 = shiftud(temp1,v_values(v),0);
        for q = 0:q_max
            % R+q cannot exceed the number of sub-blocks
            if R + q > Number_of_Blocks-1
                break
            end

            % FFT of the (R+q)'th block of S2
            temp2 = fftshift(fft([S2(1+(R+q)*N1 : N2 + N1*(R+q));...
                zeros(N2,1)]));

            % Multiplies temp1 & temp2, FFTs the product, then adds to
            % previous values for the same value of q (but different R)
            temp(:,q+1) = temp(:,q+1) + ...
                                abs(fftshift(fft(temp1.*conj(temp2))));
        end
    end

    % Each value of q was used a different # of times, so they must be
    % scaled properly.
    for q_index = 1:q_max+1
```

```
        temp(:,q_index) = temp(:,q_index) / divisors(q_index);
    end

    % If combination of current v and any q provides a greater value
    % than the previous max, then remember m, Q, & V.
    if max(max(temp))>x
        x = max(max(temp));
        [m, Q] = find(temp == max(max(temp)));

        % Must do this since q starts at 0, but Matlab doesn't allow for
        % zero indexing.
        Q = Q - 1;
        V = v_values(v);
    end
end

% Coarse estimate of TDOA (in # of samples)
TDOA_Coarse = Q * N1 + (-N2+1 + m);

% Coarse estimate of FDOA (in Freq Bin #)
FDOA_Coarse = V/N1*N;

% ********************************************************************
% FINE MODE computations.
% ********************************************************************

S2 = conj(S2);              % S2 is conjugated in basic CAF definition

% Vector of freq "bins" to use (DON'T have to be integers!!)
k_val = FDOA_Coarse-10 : FDOA_Coarse+10;

% Vectors of TDOAs to use (must be integers)
tau_val = TDOA_Coarse-10 : TDOA_Coarse+10;

done = 0;
multiple = 1;
decimal = 0;
while ~done         % Fine mode iterations continue until user is done.

    % Initialize to make later computations faster
    amb(length(k_val),length(tau_val))=0;
    Ntemp = N * multiple;
    for k = 1:length(k_val)         % Must loop through all values of k

        % Vector of complex exponentials that will be used
        exponents = exp(-1i*2*pi*k_val(k)/Ntemp*(0:Ntemp-1)');

        % Must loop through all potential TDOAs
        for t = 1:length(tau_val)

            % S2 is shifted "tau" samples
            S2temp = shiftud(S2,tau_val(t),0);

            % Definition of CAF summation
```

```
            temp = abs(sum(S1.*S2temp.*exponents));

            % Save CAF magnitude for the values of k & t
            amb(k,t)=temp;
        end
    end

    [k, t]=find(amb==max(max(amb)));     % Find the peak of the CAF matrix

    TDOA = tau_val(t);   % TDOA and FDOA associated with the peak of the
    FDOA = k_val(k);     % CAF plane. These represent the final TDOA
                         % & FDOA estimates.

    % The results are displayed.
if Ntemp >= 2^19
    disp('Maximum TDOA processing capability has been achieved.')
    doneT = 1;
else doneT = 0;
end

        done = 1;
end

        CAF_peak(S1_orig, S2_orig, floor(TDOA/multiple) - 50, ...
            floor(TDOA/multiple) + 50, (FDOA-20)/N, (FDOA+20)/N, fs);
%end
```

L

Complex Ambiguity Function Peak Value Plotting MATLAB Function

The function `CAFPeak.m` plots the peak values of the complex ambiguity function for time deviation (TDOA) and frequency deviation (FDOA). The function was developed by Johnson (2001).

Listing L.1: Complex Ambiguity Function Plot Developed By LCDR J.J.Johnson

```
 function [TDOA, FDOA, MaxAmb, Amb] = ...
CAF_peak(S1, S2, Tau_Lo, Tau_Hi, Freq_Lo, Freq_Hi, fs)

% ********************************************************************
% CAF_peak(S1, S2, Tau_Lo, Tau_Hi, Freq_Lo, Freq_Hi) takes as input:
% two signals (S1, S2) that are row or column vectors; a range of
% time delays (in samples) to search (Tau_Lo, Tau_Hi must be
% integers between -N & +N); a range of digital frequencies (in
% fractions of sampling frequency) to search (Freq_Lo, Freq_Hi must
% be between -1/2 and 1/2, or -(N/2)/N and (N/2)/N, where N is the
% length of the longer of the two signal vectors); and the sampling
% frequency, fs.
%
% The function computes the Cross Ambiguity Function of the two
% signals. Four plots are produced which represent four different
% views of the Cross Ambiguity Function magnitude versus the input
% Tau and Frequency Offset ranges.
%
% The function returns the scalars TDOA, FDOA, and MaxAmb, where
% TDOA & FDOA are the values of Time Delay and Frequency Offset
% that cause the Cross Ambiguity Function to peak at a magnitude
% of MaxAmb. Amb is the matrix of values representing the CAF
% surface.
% Written by: LCDR Joe J. Johnson, USN
% Last modified: 26 August 2001
% ********************************************************************


% Ensures that the user enters all SIX required arguments.
if (nargin < 6)
    error...
    ('6 arguments required: S1, S2, Tau_Lo, Tau_Hi, Freq_Lo, Freq_Hi');
end

% Ensures that both S1 & S2 are row- or column-wise vectors.
if ((size(S1,1)~=1) && (size(S1,2)~=1)) || ((size(S2,1)~=1) && ...
                                            (size(S2,2)~=1))
    error('S1 and S2 must be row or column vectors.');
end

N1 = length(S1);
N2 = length(S2);
S1 = reshape(S1,N1,1);      % S1 & S2 are reshaped into column-wise
```

```
S2 = reshape(S2,N2,1);      % vectors since MATLAB is more efficient
                            % when manipulating columns.

S1 = [S1;zeros(N2-N1,1)];   % Ensure that S1 & S2 are the same size,
S2 = [S2;zeros(N1-N2,1)];   % padding the smaller one w/ 0s as neeeded.

% This WHILE loop simply ensures that the length of S1 & S2 is a power
% of two. If not, the vectors are padded with 0s until their length
% is a power of two. This is not required, but it takes advantage of
% the fact that MATLAB's FFT computation is significantly faster for
% lengths which are powers of two!
while log(length(S1))/log(2) ~= round(log(length(S1))/log(2))
    S1(length(S1)+1) = 0;
    S2(length(S2)+1) = 0;
end

N = length(S1);

% Ensures that the Tau values entered are in the valid range.
if abs(Tau_Lo)>N || abs(Tau_Hi)>N
    error('Tau_Lo and Tau_Hi must be in the range -N to +N.');
end

% Ensures that Tau values entered by the user are integers.
if (Tau_Lo ~= round(Tau_Lo)) || (Tau_Hi ~= round(Tau_Hi))
    error('Tau_Lo and Tau_Hi must be integers.')
end

% Ensures that the Frequency values entered are in the valid range.
if abs(Freq_Lo)>1/2 || abs(Freq_Hi)>1/2
    error('Freq_Lo and Freq_Hi must be in the range -.5 to +.5');
end

% Ensures that the lower bounds are less than the upper bounds.
if (Tau_Lo > Tau_Hi) || (Freq_Lo > Freq_Hi)
    error('Lower bounds must be less than upper bounds.')
end

% Freq values converted into integers for processing.
Freq_Lo = round(Freq_Lo*N);
Freq_Hi = round(Freq_Hi*N);

% Creates vectors for the Tau & Freq values entered by the user. Used
% for plotting...
TauValues = (Tau_Lo:Tau_Hi);
FreqValues = (Freq_Lo:Freq_Hi)/N;

% The IF statement calculates the indices required to isolate the
% user-defined frequencies from the FFT calculations below.
if Freq_Lo < 0 && Freq_Hi < 0
    Neg_Freq = (N+Freq_Lo+1:N+Freq_Hi+1);
    Pos_Freq = [];
elseif Freq_Lo < 0 && Freq_Hi >= 0
    Neg_Freq = (N+Freq_Lo+1:N);
```

```
    Pos_Freq = (1:Freq_Hi+1);
else
    Neg_Freq = [];
    Pos_Freq = (Freq_Lo+1:Freq_Hi+1);
end

% This FOR loop actually calculates the Cross Ambiguity Function for
% the given range of Taus and Frequencies. Note that an FFT is
% performed for each Tau value and then the frequencies of interest
% are isolated using the Neg_Freq and Pos_Freq vectors obtained above.
% For each value of Tau, the vector S2 is shifted Tau samples using a
% call to the separate function "SHIFTUD". Samples shifted out are
% deleted and zeros fill in on the opposite end.

% Initializing Amb with 0s makes computations much faster.
Amb=zeros(length(Neg_Freq)+length(Pos_Freq),length(TauValues));
for t = 1:length(TauValues)
    temp = fft((S1).*conj(shiftud(S2,TauValues(t),0)));
    Amb(:,t) = [temp(Neg_Freq);temp(Pos_Freq)];
end

% Only interested in the Magnitude of the Cross Ambiguity Function.
Amb = abs(Amb);

% The following will remove any spike that occurs at Tau = FreqOff = 0.
% This may be desired in some cases, especially when the spike at (0,0)
% is due to correlation of the two signals' noise components. The
% spike, of course, could also indicate that the two signals have no
% TDOA or FDOA between them.

% if find(TauValues == 0) & find(FreqValues == 0)
% Amb(find(FreqValues==0),find(TauValues==0)) = 0;
% end


% The two different views of the Cross Ambiguity Function plots are
% created here.

figure(3) % This one is the 3-D view
set(gcf, 'Position', [100 10 500 400]);
set(gcf, 'MenuBar', 'none', 'Name', '3d CAF Plot', 'NumberTitle', 'off');
surf(TauValues/fs,FreqValues*fs,Amb);
    xlabel('TDOA (Seconds)');
    ylabel('FDOA (Hertz)');
    zlabel('Magnitude');
    title('Complex Ambiguity Function');

%%This one is a 2-D view looking down on the plane
figure(4)
set(gcf, 'Position', [700 10 500 400]);
set(gcf, 'MenuBar', 'none', 'Name', '2D CAF Plot', 'NumberTitle', 'off');
pcolor(TauValues/fs,FreqValues*fs,Amb);
    xlabel('TDOA (Seconds)');
    ylabel('FDOA (Hertz)');
```

```
    zlabel('Magnitude');
    title('Complex Ambiguity Function');
    view(0,90);

% Finds the indices of the peak value.
[DFO, DTO] = find(Amb==max(max(Amb)));
TDOA = TauValues(DTO);  % Finds the actual value of the TDOA.
FDOA = FreqValues(DFO); % Finds the actual value of the FDOA.
MaxAmb = max(max(Amb)); % Finds the actual Magnitude of the peak.
```

M

GNU Radio Complex Binary Data Reading MATLAB Function

The function `Read_Complex_Binary.m` was developed by GNU Radio (GNURadio 2016*a*) to interpret data produced by GNU Radio flowgraphs in Octave or MATLAB .

Listing M.1: Complex Binary Data Processing Function

```
%
% Copyright 2001 Free Software Foundation, Inc.
%
% This file is part of GNU Radio
%
% GNU Radio is free software; you can redistribute it and/or modify
% it under the terms of the GNU General Public License as published by
% the Free Software Foundation; either version 3, or (at your option)
% any later version.
%
% GNU Radio is distributed in the hope that it will be useful,
% but WITHOUT ANY WARRANTY; without even the implied warranty of
% MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
% GNU General Public License for more details.
%
% You should have received a copy of the GNU General Public License
% along with GNU Radio; see the file COPYING.  If not, write to
% the Free Software Foundation, Inc., 51 Franklin Street,
% Boston, MA 02110-1301, USA.
%

function v = read_complex_binary (filename, count)

  %% usage: read_complex_binary (filename, [count])
  %%
  %%  open filename and return the contents as a column vector,
  %%  treating them as 32 bit complex numbers
  %%

  m = nargchk (1,2,nargin);
  if (m)
    usage (m);
  end

  if (nargin < 2)
    count = Inf;
  end

  f = fopen (filename, 'rb');
  if (f < 0)
    v = 0;
  else
    t = fread (f, [2, count], 'float');
    fclose (f);
    v = t(1,:) + t(2,:)*i;
```

```
  [r, c] = size (v);
  v = reshape (v, c, r);
end
```

N

Passive Bistatic Radar Data Windowing MATLAB Program

The function `ERP2016Processing.m` processes the radar data collected at a test location, and breaks it into appropriately sized windows for calculation in the Complex Ambiguity Function.

Listing N.1: Raw Data Processing and Windowing Program

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% ERP2016: Engineering Research Project 2016                            %
% Passive Radar Processing                                              %
% Data Window Processing                                                %
% Compiled 20 July 2016                                                 %
% Student Name: Mathew Ryan                                             %
% Student ID: 0061010502                                                %
% File Title: ERP2016_Processing.m                                      %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


%% PROGRAM DESCRIPTION
%  Program to window data for processing through the complex
% ambiguity function


%% RESET MATLAB ENVIRONMENT
clear all
close all


%% LOAD RECORDED DATA
ReferenceSig = read_complex_binary('DopplerCh0.cfile');
SurveillanceSig = read_complex_binary('DopplerCh1.cfile');
CentreFreq = 433.050e6;%177.5e6;
Fs = 500000;%2e6;


%% DETERMINE TOTAL NUMBER OF SAMPLES IN EACH VECTOR
ReferenceSigLength = length(ReferenceSig);
SurveillanceSigLength = length(SurveillanceSig);


%% DETERMINE OVERALL VECTOR SIZE
if ReferenceSigLength <= SurveillanceSigLength
    OverallLength = ReferenceSigLength;
else if SurveillanceSigLength < ReferenceSigLength
        OverallLength = SurveillanceSigLength;
    end
end

%% TRUNCATE VECTORS TO EQUAL LENGTH
ReferenceSig(OverallLength+1:end)=[];
```

```
SurveillanceSig(OverallLength+1:end)=[];


%% INTEGRATION WINDOW
% samples to process per window
WindowLen = Fs/4;


%% COLLECTED DATA DETAILS
RecordLength = OverallLength/Fs;
WindowAperture = Fs/WindowLen;

%% NUMBER OF FRAMES
NumWindows = floor(OverallLength/WindowLen);


%% DISPLAY DATA STATITICS
fprintf(1, 'Total Length = %d Samples, Using %d Samples/Window, Total Windows = %d\n', ...
            OverallLength, WindowLen, NumWindows);
fprintf(1, 'Total Time = %f Seconds, Using %d Windows/Second\n', ...
            RecordLength, WindowAperture);


%% -------- PROCESS DATA ONE INTEGRATION WINDOW AT A TIME --------------


%% ALLOCATE THE TIME-FREQUENCY SPECTRUM
TimeSpec = zeros(NumWindows, WindowLen);


%% RESET WINDOW POINTER
WindowStart = 1;


for WindowNum = 1:NumWindows
    fprintf(1, 'Processing Window %d of %d\n', WindowNum, NumWindows);


    %% EXTRACT THE WINDOW OF I/Q SAMPLES
    RefWindow = ReferenceSig(WindowStart:WindowStart+WindowLen-1);
    SurWindow = SurveillanceSig(WindowStart:WindowStart+WindowLen-1);

    %% CODE HERE


    %% DETERMINE WINDOW CORRELATION
    [acorr,lag]=xcorr(RefWindow,SurWindow);
    [~,I] = max(abs(acorr));
    lagDiff = lag(I);
    timeDiff = lagDiff/Fs;
    fprintf(1, 'Lag: %d Samples, %d Seconds\n', lagDiff, timeDiff);


    %% PLOT FFT OF REFERENCE SIGNAL WINDOW
```

```
p=fftshift(fft(RefWindow)); %find FFT
z = 20*log10(abs(p)/max(abs(p))); %normalize

Low_freq=(CentreFreq-Fs/2); %lowest frequency to plot
High_freq=(CentreFreq+Fs/2); %highest frequency to plot

N=length(z);
freq=[0:1:N-1]*(Fs)/N+Low_freq;

figure(1);
plot(freq,z);
axis tight
set(gcf, 'Position', [100 150 500 400]);
set(gcf, 'MenuBar', 'none', 'Name', 'FFT of Reference Signal Window',...
    'NumberTitle', 'off');
xlabel('Freqency [MHz]','FontSize', 14)
ylabel('Relative amplitude [dB down from max]','FontSize', 14)
grid on
set(gcf,'color','white');

title({'Reference Signal Spectrum',['Center frequency = ' ...
    num2str(CentreFreq) ' MHz'] },'FontSize', 14)

%Add vertical line
y1=get(gca,'ylim');
hold on;
plot([CentreFreq CentreFreq],y1,'r-','linewidth',2);
hold off;
drawnow;


%% PLOT FFT OF SURVEILLANCE SIGNAL WINDOW
p=fftshift(fft(SurWindow)); %find FFT
z = 20*log10(abs(p)/max(abs(p))); %normalize

Low_freq=(CentreFreq-Fs/2); %lowest frequency to plot
High_freq=(CentreFreq+Fs/2); %highest frequency to plot

N=length(z);
freq=[0:1:N-1]*(Fs)/N+Low_freq;

figure(2);
plot(freq,z);
axis tight
set(gcf, 'Position', [700 150 500 400]);
set(gcf, 'MenuBar', 'none', 'Name', 'FFT of Surveillance Signal Window',...
    'NumberTitle', 'off');
xlabel('Freqency [MHz]','FontSize', 14)
ylabel('Relative amplitude [dB down from max]','FontSize', 14)
grid on
set(gcf,'color','white');

title({'Surveillance Signal Spectrum',['Center frequency = '...
    num2str(CentreFreq) ' MHz'] },'FontSize', 14)
```

```
    %Add vertical line
    y1=get(gca,'ylim');
    hold on;
    plot([CentreFreq CentreFreq],y1,'r-','linewidth',2);
    hold off;
    drawnow;


    %% CAF PLOT
    [TDOA, FDOA] = CAF(RefWindow,RefWindow,20,Fs,1);
    saveas(figure(3),sprintf('Radar/3D_Window_%d.png',WindowNum));
    saveas(figure(4),sprintf('Radar/2D_Window_%d.png',WindowNum));


    %% DELAY TO MATCH SAMPLE PROCESSING RATE
    %pause(0.25);


    %% POINT TO NEXT FRAME IN BUFFER
    WindowStart = WindowStart + WindowLen;


end
```

0

Digital Storage Oscilloscope Calibration Certification

CELEMETRIX
the art of measurement

Celemetrix Australia Pty Ltd
Unit 1, 6 Anella Ave
Castle Hill, NSW 2154

NATA Accredited
Laboratory Number 19397

Certificate of Calibration

QA-NMS 001

Calibration Certificate Number: M410769/3AL

UNIT UNDER TEST:	Tektronix TDS3034C Oscillosope	TEMPERATURE:	23°C ± 5°C
SERIAL NUMBER:	C014478	HUMIDITY:	50% ± 30% RH
OPTIONS:		CALIBRATED BY:	Kevin Fraser
PROCEDURE NAME:	Tek_TDS3054C_Cal_V1.32_D_SydAcc_ClosedLoop_14092015	PROCEDURE REV:	V1.32
		ASSET NUMBER:	A74086
CUSTOMER:	Department of Defence Building L474-2ND floor RAAF Williams Laverton, VIC 3028	CMX BARCODE:	CMX107980
		CAL DATE:	29/02/2016
		DUE DATE:	28/02/2017

REPORT TYPE: AS-LEFT

This Certificate of Calibration applies only to the item being calibrated, identified above and shall not be reproduced, except in full, unless written permission for an approved abstract is obtained from Celemetrix Australia Pty Ltd.

Accredited for compliance with ISO/IEC 17025. NATA is a signatory to the ILAC mutual recognition agreement for the mutual recognition of the equivalence of testing, calibration and inspection reports.

Measurements in this calibration are traceable to the International System of Units (SI) via national metrology institutes that are signatories to the CIPM Mutual Recognition Agreement.

The report may contain data that is not within the Scope of Accreditation. The unaccredited material is indicated by an Asterisk (*) in the Expanded Measurement Uncertainty field (Exp Uncert) adjacent to the affected parameter. NATA accreditation does not cover the performance of this service.

Measurement uncertainties at the time of test, expressed in SI units, are given on the following pages, where applicable. They are calculated in accordance with the methods described in applicable Guides to the Uncertainty in Measurement (GUM), using a coverage factor k=2.0, corresponding to a confidence level of 95%.

Evaluation of Results:
One or more test result values are within specification but when including the measurement uncertainty range may exceed the specification limits - **One or more test points has a result of Pass Indeterminate**

As-Left Data Type Definition: Calibration data collected after adjustment or repair. For As-Found condition results please refer to Calibration Certificate number M410769/3AF, unless otherwise noted in remarks.

Result Definitions:

Pass:	The measured test result value (including the uncertainty range when the test point is within the Scope of Accreditation) is within the specification limits.
Pass Indeterminate:	The measured test result value is within the specification limit, but when including the uncertainty range the measurement may exceed the specification limit.
Fail Indeterminate:	The measured test result value is outside the specification limit, but when including the uncertainty range the measurement may be within the specification limit.
Fail:	The measured test result value including the uncertainty range is outside the specification limits.

Remarks: After repair.

Signed: _____ Date Of Issue: 9/3/2016

☑ Jason Dortmans
Technical Director

☐ Aarthy Sriram
Senior Technician

Date Printed: 08/03/2016

SERIAL NUMBER: C014478 **Calibration Certificate Number: M410769/3AL** Model: TDS3034C

Standards Used

Asset #	Description	Cal Date	Due Date
Instrument 62	Fluke 5520A Multi-Product Calibrator	8/12/2015	8/12/2016

SERIAL NUMBER: C014478 **Calibration Certificate Number: M410769/3AL** Model: TDS3034C

Test Results

Test Description	Test Result	Lower limit	Upper limit	Units	Result	Exp Uncert ±
IDENTIFICATION						
Serial Number:	Not available					
Firmware Level:	CF:91.1CT FV:v4.26 TDS3GV:v1.00 TDS3FFT :v1.00 TDS3TRG:v1.00					
SIGNAL PATH COMPENSATION					Pass	*
SELF TEST					Pass	*
DC VOLTAGE MEASUREMENT ACCURACY						
Channel 1						
1 mV/div, 100 mV input	99.96	99.25	100.80	m V	Pass	1.03E-004 V
2 mV/div, -7 mV input	-7.125	-7.540	-6.460	m V	Pass	4.96E-005 V
5 mV/div, -100 mV input	-100.15	-101.80	-98.24	m V	Pass	1.03E-004 V
50 mV/div, 1 V input	0.9984	0.9824	1.0180	V	Pass	6.22E-004 V
50 mV/div, 650 mV input	649.1	632.4	667.6	m V	Pass	4.22E-004 V
50 mV/div, 350 mV Delta	349.4	340.5	359.5	m V	Pass	*
90 mV/div, -315 mV input	-317.2	-339.3	-290.7	m V	Pass	2.33E-004 V
200 mV/div, 10 V input	9.995	9.900	10.100	V	Pass	6.00E-003 V
1 V/div, -10 V input	-9.943	-10.300	-9.698	V	Pass	6.00E-003 V
Channel 2						
1 mV/div, 100 mV input	99.93	99.25	100.80	m V	Pass	1.03E-004 V
2 mV/div, -7 mV input	-7.091	-7.540	-6.460	m V	Pass	4.96E-005 V
5 mV/div, -100 mV input	-100.05	-101.80	-98.24	m V	Pass	1.03E-004 V
50 mV/div, 1 V input	0.9984	0.9824	1.0180	V	Pass	6.22E-004 V
50 mV/div, 650 mV input	649.7	632.4	667.6	m V	Pass	4.22E-004 V
50 mV/div, 350 mV Delta	348.6	340.5	359.5	m V	Pass	*
90 mV/div, -315 mV input	-316.6	-339.3	-290.7	m V	Pass	2.33E-004 V
200 mV/div, 10 V input	9.995	9.900	10.100	V	Pass	6.00E-003 V
1 V/div, -10 V input	-9.932	-10.300	-9.698	V	Pass	6.00E-003 V
Channel 3						
1 mV/div, 100 mV input	100.01	99.25	100.80	m V	Pass	1.03E-004 V
2 mV/div, -7 mV input	-7.041	-7.540	-6.460	m V	Pass	4.96E-005 V
5 mV/div, -100 mV input	-100.10	-101.80	-98.24	m V	Pass	1.03E-004 V
50 mV/div, 1 V input	0.9988	0.9824	1.0180	V	Pass	6.22E-004 V
50 mV/div, 650 mV input	649.5	632.4	667.6	m V	Pass	4.22E-004 V
50 mV/div, 350 mV Delta	349.4	340.5	359.5	m V	Pass	*
90 mV/div, -315 mV input	-316.4	-339.3	-290.7	m V	Pass	2.33E-004 V
200 mV/div, 10 V input	9.995	9.900	10.100	V	Pass	6.00E-003 V
1 V/div, -10 V input	-9.966	-10.300	-9.698	V	Pass	6.00E-003 V
Channel 4						
1 mV/div, 100 mV input	100.12	99.25	100.80	m V	Pass	1.03E-004 V
2 mV/div, -7 mV input	-7.013	-7.540	-6.460	m V	Pass	4.96E-005 V
5 mV/div, -100 mV input	-100.06	-101.80	-98.24	m V	Pass	1.03E-004 V
50 mV/div, 1 V input	0.9993	0.9824	1.0180	V	Pass	6.22E-004 V
50 mV/div, 650 mV input	649.7	632.4	667.6	m V	Pass	4.22E-004 V
50 mV/div, 350 mV Delta	349.4	340.5	359.5	m V	Pass	*
90 mV/div, -315 mV input	-315.6	-339.3	-290.7	m V	Pass	2.33E-004 V
200 mV/div, 10 V input	10.002	9.900	10.100	V	Pass	6.00E-003 V

SERIAL NUMBER: C014478 **Calibration Certificate Number: M410769/3AL** Model: TDS3034C

Test Results

Test Description	Test Result	Lower limit	Upper limit	Units	Result	Exp Uncert ±
1 V/div, -10 V input	-9.973	-10.300	-9.698	V	Pass	6.00E-003 V
BANDWIDTH						
Channel 1						
212.0 mV @ 500 MHz	157.7	150.0	212.0	m V	Pass Indeterminate	1.06E-002 V
Channel 2						
212.0 mV @ 500 MHz	151.7	150.0	212.0	m V	Pass Indeterminate	1.06E-002 V
Channel 3						
212.0 mV @ 500 MHz	156.6	150.0	212.0	m V	Pass Indeterminate	1.06E-002 V
Channel 4						
212.0 mV @ 500 MHz	155.8	150.0	212.0	m V	Pass Indeterminate	1.06E-002 V
TRIGGER SENSITIVITY AT FULL BANDWIDTH						
Channel 1						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
Channel 2						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
Channel 3						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
Channel 4						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
TRIGGER SENSITIVITY AT 50 MHZ						
Channel 1						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
Channel 2						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
Channel 3						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
Channel 4						
Rising Slope, Stable Trigger					Pass	*
Falling Slope, Stable Trigger					Pass	*
SAMPLE RATE AND DELAY TIME ACCURACY						
Limit : ±2 div @1 µs/div, 100 ms delay time					Pass	*

***** End of Certificate *****